Chaos Computer Club
Constanze Kurz
Felix Lindner, Frank Rieger, Thorsten Schröder

Stellungnahme

anläßlich der Verfassungsbeschwerde gegen den § 202c StGB

Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit

15. Juli 2008

Inhaltsverzeichnis

1 Zweck einer Software

Das Ziel des Gesetzgebers, bestimmte Programme aus dem Verkehr zu ziehen, um Straftaten verhindern, wird in der vorliegenden Norm dadurch zu erreichen versucht, daß auf den Zweck einer Software abgestellt wird. In der Begründung des Gesetzesentwurfes heißt es dazu, daß die Software „in ersten Linie dafür ausgelegt oder hergerichtet worden ist, bestimmte Computerstraftaten zu begehen“.[1] Entscheidend soll hier also eine objektiv mögliche Zweckbestimmung sein und eben gerade nicht der Zweck, den der Benutzer einem Programm subjektiv gibt. Es geht also um solche „Programme, denen die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind“.[2]

Der Zweck eines Computerprogramms kann in keinem Fall mit ausschließlich informationstechnischen Mitteln bestimmt werden. Wäre dies der Fall, so gäbe es perfekte Sicherheitsprogramme zur Erkennung von Schadsoftware (z. B. Anti-Viren-Programme). Würde eine informationstechnische Bestimmung des Zwecks eines Programms möglich sein, so wäre diese heutzutage in jedem Computer vorhanden und würde automatisch Schadsoftware erkennen und abwehren. Das Fehlen eines solchen Mechanismus heute deutet auch in Zukunft auf die Unmöglichkeit der Bestimmbarkeit des Zwecks einer Software hin.

Der Zweck eines Computerprogramms leitet sich in der Praxis stets aus dem situativen Kontext ab, in welchem die Software verwendet wird. Der Gesetzgeber hat also besonders den Umgang mit „dual use“-Programmen nicht klar geregelt. Wie wir im Folgenden erläutern werden, liegen die Auslegungsprobleme der neuen Norm und mithin die Unsicherheiten in der Wirtschaft, in der Forschung und bei privaten Anwendern bereits jetzt auf der Hand.

Durch die Schaffung des derzeit rechtskräftigen umstrittenen Paragraphen im StGB entstand größte Unsicherheit bei allen Beteiligten, Unternehmen, Forschern und Arbeitnehmern, zumal die Forschungstätigkeit in der IT-Sicherheitsbranche oftmals nicht nach Feierabend in der Firma endet, sondern im Kopf und auf dem Laptop eines Mitarbeiters weiter fortgeführt wird.

1.1 Werkzeuganalogie

Computerprogrammen einen eindeutigen Zweck zuordnen zu wollen, ist genausowenig möglich, wie einem mechanischen Werkzeug einen eindeutigen Zweck zusprechen zu wollen. Beispielhaft kann man solche „dual use“-Software mit in der realen Welt vorkommenden Werkzeugen vergleichen. So ist etwa ein Skalpell ein typischerweise von Ärzten verwendetes Präzisionswerkzeug, kann in der Hand von Kriminellen jedoch zur Waffe werden.

Der Besteckkasten eines Chirurgen enthält neben dem Skalpell eine große Zahl weiterer Instrumente. Man könnte mit ihnen neben dem intendierten Zweck schwere Verletzungen und Verstümmelungen an Menschen verur-

---

[1] Anlage 1 von BT-Drucksache 16/3656, S. 11.

[2] Gegenäußerung der Bundesregierung, Anlage 3 von BT-Drucksache 16/3556, S. 19.

sachen, Organe für den Weiterverkauf entnehmen oder gezielt große Schmerzen zufügen. Ein Skalpell kann, für sich alleine betrachtet, dazu dienen, Verbrechen zu begehen. Es kann aber eben auch dazu verwendet werden, Menschenleben zu retten, Tumore zu entfernen und Verletzungen zu operieren. Niemand würde jedoch auf die Idee kommen, die möglichen verbrecherischen Anwendungen von chirurgischen Werkzeugen zum Anlaß für ein generelles gesetzliches Verbot des Einsatzes, der Weiterentwicklung oder des Verkaufs zu nehmen.

Dieses Beispiel aus dem medizinischen Bereich läßt sich auf viele weitere Lebenssachverhalte übertragen. Ob etwa ein Hammer ein einfaches Werkzeug oder ein Tatmittel eines Mordes ist, läßt sich eben nicht ohne Betrachtung des Kontextes feststellen.

Selbst wenn man für einen Moment der falschen Annahme folgte, daß es Computerprogramme gäbe, die ausschließlich und eindeutig einem bestimmten kriminellen Zweck dienten, ließe sich daraus natürlich noch keine Aussage über die tatsächliche Verwendung der Software durch den Benutzer herleiten.

Als weiteres Beispiel aus der nicht-elektronischen Welt seien Schloßöffnungswerkzeuge angeführt. Diese Werkzeuge wurden speziell und mit großem Aufwand entwickelt, um Schließsysteme zerstörungsfrei zu öffnen. Man könnte nun folgern, daß diese Werkzeuge verboten werden müßten, da es bei oberflächlicher Betrachtung ihr alleiniger Zweck ist, die Öffnung einer Tür ohne den dafür vorgesehenen Schlüssel vorzunehmen. Dies impliziert eine illegale Handlung.

Diese Werkzeuge werden jedoch weitaus überwiegend von Schlüsseldiensten, technischen Hilfsdiensten oder Rettungsdiensten erworben und verwendet, um Menschen in Notlagen zu helfen. Eine weitere Gruppe von Käufern (und auch Produzenten) solcher Werkzeuge sind Privatpersonen, die sich für die Sicherheit von Schließsystemen interessieren. Sie analysieren die Funktionsweise der Schlösser, tragen sportliche Wettbewerbe im Schloßöffnen aus und erarbeiten aus den dabei gewonnenen Erkenntnissen – oft in Zusammenarbeit mit dem Schloßherstellern – Verbesserungen für die Sicherheit der Schlösser.

Ein Verbot solcher Schloßöffnungswerkzeuge aufgrund der Tatsache, daß sie neben den vielen legalen und nützlichen Anwendungsfeldern auch für Straftaten verwendet werden können, wäre unverhältnismäßig. Im Alltag wird das Mitführen solcher Werkzeuge zwar in bestimmten Situationen ein Verdachtsmoment sein, jedoch sinnvollerweise nicht für sich genommen eine Strafverfolgung rechtfertigen.

Computersicherheitswerkzeuge weisen ein ähnlich vielfältiges Anwendungsspektrum wie chirurgische Instrumente oder Schloßöffnungswerkzeuge auf. Die rechtliche Bewertung ihrer konkreten Anwendung ist daher nur im Gesamtkontext der Benutzung möglich. Eine simplifizierende Betrachtung unter einem bestimmten Blickwinkel, wie sie im § 202c StGB vorgenommen wurde, greift notwendigerweise zu kurz und führt in der Praxis zu einer Überkriminalisierung.

Auch im virtuellen Kontext finden sich Analogien: So ist etwa Google die mit Abstand meistbenutzte Suchmaschine, gleichzeitig jedoch ein unersetzbares Werkzeug, um z. B. die Verbreitung von Sicherheitslücken bei Webservern zu untersuchen. Zusätzlich bietet Google eine Liste von sog.

Phishing Sites an (siehe Kapitel 2.2). Diese Liste wird wesentlich durch Google-Benutzer gespeist, die Phishing-Webseiten melden.[3] Auch andere Anbieter bieten ähnliche Services an.[4] Die angebotenen Listen können jedoch gleichzeitig als angreifbare Computer aufgefaßt werden, auf denen man beispielsweise eigene sogenannte Phishing Kits installieren kann. Dies wird in der Praxis auch tatsächlich durchgeführt (siehe Kapitel 2.4).

Im Folgenden belegen weitere konkrete Beispiele die Unentscheidbarkeit des Zwecks eines Programms ohne Betrachtung der äußeren Umstände.

1.2 Beispiel Portscanner

Die wohl am häufigsten verwendete Klasse von Programmen zur potentiellen Vorbereitung eines Angriffs auf einen Computer sind sogenannte Portscanner. Diese Programme ermitteln das Vorhandensein von Netzwerkdiensten auf einem Computersystem. Hierfür testet der Portscanner alle Dienste eines Rechners oder einer ganzen Rechnergruppe: Maximal 131.070 mögliche Ports (je 65.535 statusbehaftete und statuslose) werden abgefragt. Mit Hilfe der Antworten wird „erraten“, ob der gesuchte Dienst verfügbar ist. Das Scannen mittels eines sog. Portscanners ist also der Versuch, durch automatisiertes Testen herauszufinden, welche Dienste auf einem Computersystem laufen. Entsprechend können also die Angriffsflächen des Computers ermittelt werden.

Exakt die gleiche Funktion wird auch von benutzerfreundlichen Betriebssystemen angeboten und verwendet, um erreichbare Computer in der unmittelbaren Nachbarschaft, beispielsweise im Heimnetz, zu ermitteln. Auch in diesem Anwendungsfall werden Anfragen an jeden bekannten Computer im Heimnetz gesendet. Aus informationstechnischer Sicht kann kein Unterschied zwischen den Funktionen beider Programme festgestellt werden.

Ein passender Vergleich in der realen Welt ist der Hausbesitzer, der vor der Fahrt in den Urlaub um sein Haus geht, um an allen Türen und Fenstern zu rütteln, um zu prüfen, ob sie auch sicher verschlossen sind. Das Installieren von guten Schlössern und Alarmanlagen gibt ihm keine Gewißheit darüber, ob nicht vielleicht doch eine Kellerluke offensteht oder ein Fenster nur angelehnt ist. Er vergewissert sich also, indem er wie ein Einbrecher vorgeht, der nach einer Schwachstelle sucht, durch die er eindringen kann. Wenn es sich um ein Gebäude handelt, das besonderen Sicherheitsstandards unterliegt, wird er auch testen, inwieweit die getroffenen Sicherheitsmaßnahmen gegen Einbruchsversuche mit Werkzeugen standhalten. Zu solchen Maßnahmen sind sowohl Hausbesitzer als auch Unternehmen im übrigen von ihrer Versicherung angehalten, sie dienen nicht nur dem Selbstschutz.

Ebenso geht ein verantwortlicher Systembetreiber vor, um sich zu vergewissern, daß sein IT-System zumindest gegen die bisher bekannten Schwachstellen gesichert ist. Er versetzt sich in die Perspektive eines Angreifers und versucht sich mit dessen Denkweise und den einem Angreifer zur Verfügung stehenden Informationen und Angriffswerkzeugen Zugang

---

[3] Eine extra von Google eingerichtete Webseite ermöglicht es jedem Benutzer, Phishing-Webseiten direkt zu melden, siehe http://tinyurl.com/rum5q vom 8. Juli 2008.

[4] Vgl. http://www.phishtank.com/ vom 8. Juli 2008.

zum System zu verschaffen. Aufgrund datenschutzrechtlicher Bestimmungen kann er zu einem solchen Vorgehen auch verpflichtet sein.

Am Beispiel eines Portscanners wird ebenfalls klar, warum es keine Software geben kann, die jede „Schadsoftware“ anhand ihrer Funktionalität detektiert. Die Vorbereitung eines Angriffs und die Suche nach erreichbaren Computer im Heimnetz sind funktional identisch.

Die Unmöglichkeit der informationstechnischen Unterscheidung spiegelt sich vor allem in größeren Unternehmensnetzwerken wider. Dort werden sogenannte heuristische Verfahren verwendet, um mögliche Angriffe frühzeitig zu erkennen. Da Unternehmensnetzwerke aber üblicherweise eine Vielzahl von Computern und Teilnetzwerken beinhalten, wird dort auch Netzwerkmanagement-Software verwendet, um die sich ständig ändernde interne Computerlandschaft zu überwachen und zu dokumentieren. Diese Systeme wiederum müssen genau die gleichen Mittel nutzen wie die vermeintlich bösartigen Portscanner, was regelmäßig zu Fehlalarmen führt und ein bis heute ungelöstes Problem darstellt.

Das Beispiel des Portscanners zeigt, daß der Zweck eines Programms mit informationstechnischen Mitteln nicht zu entscheiden ist. Einzig und allein die äußeren Umstände wie der Bediener des Programms und die Nutzung der gewonnenen Informationen können Aufschluß über den Zweck geben. Ein solches Scanning mittels Portscanner ist also keineswegs immer die Vorbereitung eines Angriffs gegen den Computer, denn nicht jeder, der sich ein Gebäude von außen betrachtet, plant auch einen Einbruch.

1.3 Automatisierte Sicherheitstests

Für die Betreiber computerisierter Systeme ist die Verwendung von Angriffswerkzeugen für die Durchführung testweiser Angriffe unerläßlich. Dabei kann es sich zunächst um einfache Werkzeuge, wie sie in jedem modernen Betriebssystem vorinstalliert sind, handeln. Insbesondere bei Unix-ähnlichen Betriebssystemen gehören Anwenderprogramme, die man als „Hackertools“ bezeichnen könnte, zum Standardumfang des Betriebssystems. Für die tägliche Arbeit von Netzwerkadministratoren und Sicherheitsexperten sind diese dringend notwendig.

Weiterhin kommen aber auch komplexe Sammlungen nahezu aller bekannten Angriffswerkzeuge zum Einsatz. Diese sind auch als „Vulnerability Scanner“[5] oder Baukastensysteme bekannt. Typische Beispiele für diese Werkzeuge sind die Programme MetaSploit und Core Impact. Sie enthalten viele hundert einzelne kleine Programme oder Module, die jeweils eine spezifische Schwachstelle angreifen. Ein Steuermodul wählt nach einer vorprogrammierten Logik entsprechend dem zu testenden System die Angriffsprogramme aus und probiert sie nacheinander durch. Dadurch kann der Systembetreiber in kurzer Zeit einen Überblick über die auf seinem System vorhandenen Schwachstellen gewinnen und diese schließen. Der Benutzer muß dazu nicht über tiefgreifende Kenntnisse verfügen.

Solche Werkzeuge lassen sich natürlich auch für die Vorbereitung und Durchführung eines Angriffs verwenden. Sie sammeln in automatisierter Weise Informationen über ausnutzbare Schwachstellen, die angegriffen werden können. Dabei ist aus technischen Gründen das Erkennen mögli-

[5] In deutsch etwa: Schwachstellen-Abtaster.

cher Angriffspunkte oft nur möglich, indem auch tatsächlich versucht wird, eine potentielle Sicherheitslücke aktiv auszunutzen.

1.4 Beispiel Debian Linux

Ein deutliches Beispiel für den nicht eindeutig bestimmbaren Zweck von potentiell schädlichen Programmen oder Daten zeigte sich in jüngster Vergangenheit. Debian ist eine der weltweit am weitesten Verwendung findenden Distribution des beliebten Open-Source-Betriebssystems Linux. In Debian Linux, ebenso wie in den weitverbreiteten Ubuntu-Distributionen, wurde im Mai 2008 eine für fast zwei Jahre offenstehende Sicherheitslücke dramatischen Ausmaßes identifiziert. Sicherheitsexperten hatten eine Schwachstelle im Zufallszahlengenerator entdeckt.[6] Das Betriebssystem hatte aufgrund eines Fehlers die Ausgangsdaten für die Erstellung von kryptographischen Schlüsseln falsch – nämlich vorhersagbar – generiert. Ist der kryptographische Schlüssel für eine Verschlüsselung bekannt, ist deren gesamte Sicherheit hinfällig.

Die Sicherheit solcher Schlüssel basiert wesentlich auf den zufälligen Ausgangsdaten, welche für die Erstellung der Schlüssel verwendet werden. Sind diese Daten vorhersagbar, so ist auch der resultierende Schlüssel ohne großen Aufwand in einfacher Weise vorherzusagen und bietet damit keinen Schutz mehr. Im Falle von Debian Linux wurde eine fehlerhafte Veränderung vorgenommen, die durch mangelnde Prozesse unentdeckt blieb. Diese Veränderung bewirkte, daß vorher zufällige Werte nun einen extrem kleinen Wertebereich hatten und damit trivial vorhersagbar wurden: Aus der ursprünglich ungeheuer großen Anzahl von möglichen Schlüsseln blieben damit nur 32.768 übrig.

Aus diesen unsicheren Ausgangsdaten wurden nun fast zwei Jahre lang Schlüssel für verschiedene Anwendungen erstellt. Hierzu zählen Schlüssel für den Zugang zu Computern als sicherer Ersatz für Paßwörter, für den Schutz von sicheren Webseiten zum Online-Einkauf oder für den Schutz von Online-Banking-Webseiten.

Ob ein Computer oder eine sichere Webseite nun von dem Problem betroffen ist, kann nur ermittelt werden, indem alle 32.768 möglichen unsicheren Schlüssel errechnet und die ermittelten Werte mit dem zu prüfenden Schlüsseln verglichen werden. Das umgekehrte Vorgehen ist aufgrund der kryptographischen Eigenschaften solcher Schlüssel unmöglich.

Fatal daran ist, daß nach der Gesetzesänderung des § 202 StGB der Besitz und die Erstellung von Paßwortlisten jeder Art unter Strafe gestellt wurde, sobald dies der Vorbereitung einer Straftat dient. Das „Hackertool“ ist in diesem Fall faktisch die Liste der Schlüssel. Die Errechnung von möglichen Schlüsseln für die Webseite beispielsweise einer Online-Bank würde wohl bei naiver Betrachtung eindeutig die Vorbereitung einer Straftat darstellen. Tatsächlich jedoch hat nur dieses (potentiell gesetzeswidrige) Verhalten von aufmerksamen Bürgern dazu geführt, daß einige betroffene Banken und Unternehmen über ihre schwachen Schlüssel unterrichtet und zum sofortigen Austausch dieser veranlaßt werden konnten.

Ungeachtet dessen sind hunderttausende Computer auf der ganzen Welt vom Problem durch den Fehler in Debian Linux betroffen. Um schnell Ab-

---

[6] Siehe Ubuntu Security Notice USN-612-2,
http://www.ubuntu.com/usn/usn-612-2 vom 12. Juli 2008.

hilfe zu schaffen, wurde von den Anbietern des Debian Linux eine Liste aller 32.768 möglichen Schlüssel zur Verfügung gestellt und die Benutzer gleichzeitig ermahnt, schnellstmöglich eine automatische Prüfung ihrer eigenen Schlüssel durchzuführen. Nach geltendem Recht ist dies aber für alle deutschen Nutzer von Debian nicht mehr eindeutig legal, da sie über die automatische Prüfung genau diese Liste von möglichen Zugangsschlüsseln erhalten, die sie auch für den Einbruch in fremde betroffene Computer nutzen könnten.

Jedem Debian Linux, welches seit dem Bekanntwerden des Sicherheitsproblems installiert wurde, liegt zudem heute unaufgefordert eine solche Liste der unsicheren Zugangsschlüssel bei. Dies ermöglicht es, den Benutzer zu warnen, wenn er einen alten, unsicheren Schlüssel verwenden will. Viele Benutzer behalten ihre Schlüssel über Jahre, da deren Sicherheit als deutlich höher als die von Paßwörtern eingestuft wird und sie daher nicht so oft gewechselt werden.

Es ist für einen Benutzer unmöglich nachzuweisen, daß die Liste der unsicheren Schlüssel ausschließlich für den Zweck der Sicherheit des eigenen Computers vorhanden ist. Es handelt sich also faktisch immer um eine gesetzeswidrige Liste von Zugangsdaten. Ohne diese Liste ist aber die Sicherheit eines Computers nicht zu gewährleisten, da die Benutzer des Computers ihren Schlüssel in den meisten Fällen verwenden, um mit dessen Hilfe Zugang zum System zu erhalten. Kann der legitime Besitzer des Computers die eingereichten Schlüssel nicht auf ihre Sicherheit überprüfen, so riskiert er einen erfolgreichen Einbruch in das Benutzerkonto eines betroffenen Benutzers. Entsteht daraufhin aus dem erfolgreichen Einbruch ein Schaden, zum Beispiel durch von dem Computer aus durchgeführte weitere Angriffe, so ist der Besitzer des Computers in den meisten Fällen für das fahrlässige Verhalten, den Schlüssel nicht zu prüfen, zivilrechtlich haftbar.

Anhand der dargelegten Beispiele wird deutlich, daß es unmöglich ist, einen eindeutigen Zweck einer Software oder einer Datensammlung zu bestimmen. Eine Liste mit schwachen Schlüsseln oder Standard-Paßwörtern ist sowohl für Sicherheitstests als auch für Angriffe gegen Computersysteme verwendbar. Softwarewerkzeuge, die für den normalen Betrieb eines Systems notwendig sind, lassen sich ebenso für Angriffe wie für Sicherheitstests verwenden.

2 Besitz und Analyse von Schadsoftware

Für die Verbesserung der Sicherheit heutiger und zukünftiger Computer und Software ist es unerläßlich, Schadsoftware und Angriffsprogramme zu besitzen und detailliert zu analysieren. Nach heutigem Stand der Technik ist es unmöglich, ein fehlerfreies komplexes Computerprogramm nicht-trivialer Größe zu erstellen.[7] Allein die Menge der an der Erstellung und Ausführung des Programms beteiligten Komponenten ist so hoch, daß Fehlerfreiheit praktisch unmöglich ist. Hinzu kommt eine unüberschaubare Interaktion der Komponenten während der Ausführung eines Programms.

Fehler in Computerprogrammen entstehen also geradezu zwangsläufig während der Erstellung des Programms in seiner ursprünglichen Form. Die hauptsächliche Problematik besteht allerdings darin, daß Fehler erst durch ihre Manifestierung als Fehlverhalten bei der tatsächlichen Benutzung und Ausführung des Programms in seiner endgültigen Form erkannt werden. Es ist mit heutigen Mitteln leider unmöglich, Fehler vorher zuverlässig als solche zu identifizieren und damit ihre Beseitigung vorab zu ermöglichen.

Manifestiert sich nun ein Fehler durch offensichtliches Fehlverhalten eines Programms, so geschieht dies nur, wenn eine große Anzahl von vorhergehenden Bedingungen erfüllt wurde. In den meisten Fällen geschieht dies zufällig auf Grund von Aktionen, die der Anwender des Programms in einer bestimmten Reihenfolge ausgeführt hat. Jedem Computeranwender ist das Verhalten bekannt, daß eine Aktion durch Auswählen einer bestimmten Sequenz von Funktionen gelingt, bei einer abweichenden Sequenz allerdings zu Fehlverhalten führt.

Doch selbst nachdem sich ein Fehler durch ein Fehlverhalten bei der Ausführung des Programms zu erkennen gegeben hat, ist es in vielen Fällen sehr schwierig, den Fehler selbst zu identifizieren. Dieses Problem bezeichnet man als Nachstellbarkeit oder Reproduzierbarkeit. Hersteller von Software haben permanent mit diesem Problem zu kämpfen, wenn bei Kunden Fehlverhalten auftreten, welche im eigenen Haus nicht nachvollzogen werden können. Da beim Kunden das Programm nur in seiner endgültigen Form in der vorhandenen Computerumgebung vorliegt, es aber in seiner ursprünglichen Form für die Auffindung des zugrundeliegenden Fehlers vorhanden sein muß, werden bei Softwareherstellern große Anstrengungen unternommen, das Fehlverhalten nachstellen und nachvollziehen zu können. Häufig sind selbst diese Anstrengungen nicht von Erfolg gekrönt. Der Einfluß von scheinbar unbedeutenden Rahmenbedingungen macht diese Aufgabe bis heute zu einer der schwierigsten im gesamten Bereich der Softwareentwicklung.

Bei Schadprogrammen handelt es sich in den meisten Fällen um die automatisierte Ausnutzung von Fehlern. Das heißt, das Schadprogramm löst gezielt einen Fehler aus und nutzt das resultierende Fehlverhalten, um eine unvorhergesehene Aktion ausführen zu können. Dabei unterliegen Schadprogramme denselben Problemen, die durch die vorhergehend beschriebene allgemeine Reproduzierbarkeit von Fehlverhalten entstehen. Auch Schadprogramme sind nur unter bestimmten Voraussetzungen in der Lage, das gewünschte Fehlverhalten auszulösen, in allen anderen Fällen schlägt der Angriff fehl. Aus diesem Grund spricht die aktuelle For-

---

[7] Computerprogramme nicht-trivialer Größe sind beispielsweise interaktive Anwendungen wie Webbrowser, Textverarbeitungsprogramme oder Betriebssysteme.

schung auf dem Gebiet der Fehlererkennung zur Verhinderung von Angriffen von „gefördertem Fehlverhalten“ (engl. „sponsored bugs“).[8]

Wie die vorangehende Erläuterung deutlich macht, kann der von einer Schadsoftware ausgenutzte zugrundeliegende Fehler nicht erkannt und behoben werden, wenn die entsprechende Schadsoftware nicht vorliegt.

2.1 Arbeitsweise in der IT-Sicherheitsbranche

Auf dem nationalen und internationalen Markt stehen sich Hersteller von IT-Sicherheitslösungen konkurrierend gegenüber. Aufgrund der hohen Verantwortung gegenüber ihren Kunden sowie auch einzelnen Anwendern in den Unternehmen sind die Softwarehersteller daher insbesondere darauf angewiesen, aktuell über neue Angriffsverfahren informiert zu sein und ihre Produkte entsprechend zeitnah anzupassen.

In den verschiedenen Segmenten des IT-Sicherheitsmarktes sind unterschiedliche Vorgehensweisen üblich, der Bedarf nach jeweils aktuellen Informationen und einer schnellen Anpassung der Funktionalitäten in der Sicherheitssoftware ist jedoch von besonderer Bedeutung. So müssen etwa Anti-Viren- oder Virenscanner-Softwarehersteller in der Lage sein, ein- und ausgehende E-Mails je nach aktuell üblichen Schadroutinen auf schadhaftes Verhalten hin zu untersuchen. Auch Hersteller von Netzwerk-Sicherheitslösungen versuchen, Einbrüche in Netzwerke zu erkennen und die automatisierte Einbruchserkennung und -abwehr[9] entsprechend anzupassen und automatisch Gegenmaßnahmen einzuleiten, um entdeckte Angriffe abzuwehren. Ebenso müssen Firewall-Hersteller bezüglich der Analyse von Schadsoftware ständig auf dem Laufenden bleiben und ihre Produkte den aktuellen Bedrohungsszenarien anpassen.

Das bedeutet, daß die Anbieter von Anti-Viren- und Sicherheitssoftware täglich an ihren Mechanismen und Erkennungsdatenbanken arbeiten müssen, um ihre Produkte zu aktualisieren. Es gehört heute für konkurrenzfähige Softwarehersteller zum Standard, täglich ein oder mehrere Aktualisierungen beispielsweise ihrer Viren-Datenbanken zu veröffentlichen.

Da die Verbreitung neuer Viren und Schadprogramme hinsichtlich des Volumens und des Schadpotentials stark schwankt, sich diese Schadsoftware aber typischerweise in regelrechten Wellen automatisiert über das Internet verbreitet, stehen Anti-Viren-Hersteller regelmäßig unter dem Druck, neu bekanntgewordenen Schädlinge zeitnah zu analysieren. Nach der Analyse müssen die entsprechenden Heuristiken zur Abwehr der Schadsoftware sofort angepaßt werden. Weiterhin werden dann die Signaturen aus der Schadsoftware extrahiert, um in der Folge die Signatur-Datenbanken anzupassen und die geänderte Datenbankversion zu verbreiten. Dies kann je nach aktuellem Aufkommen an neuen Schadroutinen sehr viel Zeit in Anspruch nehmen, da es Programmen oftmals nicht auf dem ersten Blick anzusehen ist, ob sie tatsächlich eine schadhafte Funktion ausführen.

---

[8] Vgl. K. M. Goertzel, T. Winograd, H. L. McKinley, L. Oh, M. Colon, T. McGibbon, E. Fedchak, R. Vienneau: Software Security Assurance – State-of-the-Art Report (SOAR), Defense Technical Information Center, Department of Defense, USA, 31. Juli 2007.

[9] Dies erfolgt mittels sog. Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).

Ein großer Teil der deutschen Industrie wie auch viele weitere Institutionen in der Bundesrepublik, die einem erhöhten Schutzbedarf der eigenen IT-Infrastruktur unterliegen, sind auf die beschriebenen Produktaktualisierungen der Anti-Viren-Hersteller angewiesen. Dabei stellen sie in den meisten Fällen vor allem auch die eigene Abhängigkeit von den Produkten (zum Teil ausländischer) Sicherheitsunternehmen fest. Zahlreiche große Unternehmen aus dem Bankensektor haben daher im Laufe der vergangenen Jahre eigene IT-Forschungsabteilungen aufgebaut, in denen unter anderem viele „unkonventionelle“ Sicherheitsexperten aus dem nicht-akademischen Bereich zum Einsatz kommen, um die jeweils individuellen Sicherheitsansprüche in den Unternehmen umzusetzen. Das bedeutet, daß insbesondere Banken auf eigene Kosten IT-Forschungsarbeit leisten, um speziell gegen Banken gerichtete Angriffe durch Schadsoftware abwehren zu können.

2.2 Beispiel Phishing

Beispielhaft soll hier ein Vorgehen betrachtet werden, das ein mangelndes Sicherheitsbewußtsein der Kunden ausnutzen soll, um an deren geheime Zugangsdaten zu gelangen. In der Öffentlichkeit wurde unter anderem der Begriff „Phishing“ bekannt. Der Begriff faßt Angriffsmethoden Krimineller zusammen, die ihre Opfer bei immer mehr Banken und deren Kunden suchen und das Ziel haben, an Kreditkarten- und Online-Banking-Zugangsdaten zu gelangen. Solche Angriffe gehen vornehmlich zu Lasten des Kunden. In der Regel wird bei entsprechendem Nachweis jedoch von der Bank das Geld an den Kunden zurückgezahlt. Bei Bekanntwerden solcher Angriffswellen und vor allem bei erfolgreichen Angriffen ist in jedem Fall jedoch auch die Bank die Geschädigte, da hier unter anderem ein Reputationsverlust die Folge ist, der nachhaltiger wirken kann als zurückerstattetes Geld im Falle einzelner erfolgreicher Phishing-Angriffe.

Die Vorgehensweise bei einem solchen Angriff kann vielfältig sein. Im Falle der Banken ist es zum Beispiel denkbar, daß auf dem Rechner eines Bankkunden eine Hintertür installiert wird, wobei ein Programm dafür sorgt, daß Tastatureingaben oder Netzwerkverkehr mitgelesen werden können (sog. Keylogger). Hierbei könnte auch reguläre Software der Bank ersetzt oder durch schadhafte Funktionen erweitert werden. Die ausgespähten Daten werden dann von einem Angreifer eingesammelt und zum Nachteil des Kunden mißbraucht.

Da es keine Schadsoftware geben kann, die alle Banken der Welt berücksichtigt, wenn es um das Ausspähen von Zugangs- oder Kontodaten geht, werden solche Schadprogramme in der Regel individuell für eine bestimmte Bank und deren Kunden oder Kundenkreis entwickelt. Zurückliegende Fälle zeigen, daß es hierbei keine Rolle spielt, wie groß, wichtig oder anerkannt die betroffene Bank ist: Sowohl große als auch kleinere Banken sind regelmäßig Ziel solcher Angriffe.

Genau hier zeigt sich die Schwachstelle der Abhängigkeit von Drittanbietern von Software, nämlich beispielsweise zu den Lieferanten von Anti-Viren-Softwareprodukten und den dazugehörigen Aktualisierungen. Große Anti-Viren-Hersteller können gegebenenfalls eben *nicht* individuell erstellte Schadsoftware mit besonders hoher Priorität analysieren und entsprechende Sicherheitswarnungen und Erkennungsmechanismen herausgeben.

Aus diesem Grund existieren unter anderem bei Banken eigene Abteilungen, die sich mit Sicherheitsthemen und dabei mit hoher Priorität mit Schadsoftware und Viren auseinandersetzen. Im Falle einer erneuten Flut

von solch individuell erstellter Schadsoftware via E-Mail an (potentielle) Kunden der Bank ist diese nun selbständig in der Lage, die Software und deren Funktionsweise – also deren Schadfunktionen – zu identifizieren, noch bevor es die Anti-Viren-Hersteller können.

Hierdurch ergeben sich für die Banken neue Möglichkeiten, um das allgemeine Sicherheitsniveau der Bank, der Kunden und anderer betroffener Personen zu erhöhen. Dazu können etwa Warnungen an Kunden über das eigene (Online-Banking-)Webportal herausgegeben werden, die auf eine neu in Umlauf gebrachte Schadsoftware hinweisen. Auch die Anti-Viren-Hersteller profitieren von diesen Warnungen, da eine Übermittlung detaillierter Ergebnisse der bankinternen Analyse die Arbeit der Hersteller unterstützt und somit zu einer schnelleren Verbreitung von wirksamen Gegenmaßnahmen führen kann. Gleichzeitig können die Spuren der Täter schneller verfolgt werden, um den initialen Urheber ermitteln zu können.

Insbesondere Banken profitieren also von einer vollständigen Unabhängigkeit zu Drittanbietern von Schadsoftware-Forschung. Denn sollten Anti-Viren-Hersteller – etwa aufgrund mangelnder Ressourcen – nicht sofort auf eine Anfrage eines deutschen Unternehmens reagieren, sind diese ohne eine eigene Möglichkeit der Abwehr der Gefahr machtlos und können auch keine fundierten Informationen an den eigenen betroffenen Kundenkreis weiterleiten.

Deutsche Banken, die über solche Sicherheitsabteilungen und -forscher verfügen, geraten in jedem Fall in einen Konflikt mit § 202c StGB – und hier in erster Linie die technischen Mitarbeiter. Banken haben erkannt, daß sie der anwachsenden Flut von Schadsoftware nur Herr werden können, wenn sie selbst die zum Teil individuell erstellten Programme analysieren.

Für diese Analyse ist der Besitz und Austausch von Schadprogrammen zwingend notwendig.

Das Wissen, um unter Laborbedingungen die unterschiedlichen Formen von Schadsoftware zu analysieren, läßt sich nicht in einer Universität erlernen. Hierzu gehört vielmehr die langjährige Beschäftigung mit dieser Thematik und ein unbedingt notwendiger öffentlicher Austausch mit anderen Interessierten (siehe Kapitel 2.6). Besonders Banken haben mit sehr komplexen Typen von Schadsoftware zu kämpfen, da diese Programme in der Regel mittels kryptographischer Algorithmen gegen eine Analyse geschützt und immer neue Angriffsmethoden implementiert werden, um Rechner möglichst langfristig und unerkannt mit einer Hintertür auszustatten.

Es ist im Fall einer entdeckten Schadsoftware nicht hilfreich, bei begründetem Verdacht eines gezielten Angriffs mittels einer dezidiert ausgenutzten Schwachstelle die deutschen Strafverfolgungsbehörden einzuschalten. Insbesondere gegen Angriffe über das Internet in Kombination mit sogenanntem „Social Engineering“[10] gibt es keinen schnellen behördlichen Schutz, sie erfordern jedoch ein besonders schnelles Eingreifen und Handeln, um zunächst den potentiellen Schaden eines vermeintlichen Angriffs einschätzen und abwehren zu können.

---

[10] Social Engineering bezeichnet die Ausnutzung mangelhafter Sensibilisierung von Menschen, also des „Fehlerfaktors Mensch“. Unwissentlich oder ungewollt geben Personen Informationen preis und/oder installieren wider besseres Wissen Schadsoftware.

Eine Forschungs- oder Arbeitsgruppe innerhalb eines Unternehmens, die sich auf die Analyse und Bekämpfung von Schadsoftware spezialisiert hat oder spezialisieren möchte, benötigt Freiräume bei der Wahl ihrer bevorzugt zu verwendenden Werkzeuge und Untersuchungsobjekte. Sie braucht selbstverständlich Zugriff auf „Hackertools“. Eine rechtliche Grauzone ist hierbei unangemessen und hinderlich für die Erfolgsaussichten der Forschung.

2.3 Externe IT-Sicherheitsdienstleister

Neben den Forschungsabteilungen in deutschen Unternehmen, die das Ziel anstreben, möglichst unabhängig von Anbietern von Sicherheitssoftware zu sein, existieren heutzutage weitere Abteilungen und Verantwortliche für die interne und externe IT-Sicherheit. Zur Steigerung des allgemeinen Sicherheitsniveaus eines Unternehmensnetzwerkes und ebenfalls zur Etablierung eigener Sicherheitsstandards werden häufig externe Sicherheitsdienstleister beauftragt, das Sicherheitsniveau praktisch und auch auf der Prozeßebene zu untersuchen. Die Prozeßebene bezeichnet die Definition von Richtlinien und Prozessen in Unternehmen, welche umzusetzen und fortzuführen sind, um das Sicherheitsniveau bereits auf einer konzeptuellen Ebene zu erhalten.

Zwar sind für den deutschen IT-Sicherheitsmarkt keine genauen Erhebungen bekannt, aus US-amerikanischen Befragungen sind jedoch prozentuale Zahlen dazu verfügbar, welch wichtige Bedeutung die Dienstleistungen externer Berater im Bereich IT-Sicherheit erlangt hat. So ergab eine Befragung des Computer Security Institute, daß mit 53 % in den USA über die Hälfte der befragten Unternehmen externe Dienstleister zur Evaluierung ihrer Computersicherheitsmaßnahmen beauftragen.[11] Die Zahlen für den deutschen Markt dürften vergleichbar sein. Die Branche leistet mithin einen wesentlichen Beitrag sowohl zum betrieblichen Informationsschutz als auch zum unternehmerischen Risikomanagement.

Die technischen Analysen umfassen unter anderem die Überprüfung des Soll- und Ist-Zustands eines vorab definierten Sicherheitsniveaus und der theoretischen Prozesse. Zur technischen Überprüfung der eingeführten Standards (Ist-Zustand) werden Härtungsanalysen von Systemen durchgeführt, Schwachstellen in Prozessen durch Penetration von Netzwerken und einzelnen Systemen aufgedeckt und ebenso weitere systematische Fehler identifiziert. Dies geschieht sehr individuell und entlang der Geschäftsausrichtung eines Unternehmens oder Konzerns. In vielen Fällen reicht es dabei aus, auf Werkzeuge zurückzugreifen, die allgemein nicht als sogenanntes Hacker-Werkzeug angesehen werden. Dazu gehören Webbrowser und reguläre Netzwerk-Clients, also Programme, denen in erster Linie ein durchaus friedlicher Verwendungszweck zugeschrieben wird.

Viele Werkzeuge, die für solche Analysen unabdingbar benötigt werden, sind nicht aus „offiziellen“ Quellen verfügbar. Die Gründe dafür können unterschiedlich sein. Zum einen gibt es eine immer restriktiver werdende Gesetzgebung hinsichtlich der Verwendung von „Hackertools“ in vielen Staaten. Zum anderen eröffnet sich gleichzeitig ein großer Markt für soge-

[11] Vgl. Computer Security Institute: Computer Crime and Security Survey, 2007, S. 19.

nannte „0-Days“-Exploits[12] und andere ausnutzbare Schwachstellen. Die Nicht-Veröffentlichung solcher Schwachstellen und Exploits sorgte in der vergangenen Zeit dafür, daß den Softwareherstellern weniger Schwachstellen bekanntgemacht wurden. Damit verzögerte sich jeweils die Möglichkeit, die Schwachstelle schnell zu beheben und somit einen großen Anwenderkreis abzusichern.

Für die Untersuchungen im eigenen Unternehmensnetzwerk sind solche Angriffswerkzeuge weiterhin wichtig, um zu überprüfen, ob interne Systeme identifiziert werden können, die zum Beispiel nicht mit den notwendigen Updates versehen wurden, um Schwachstellen zu schließen. Insbesondere bei umfangreichen Computernetzwerken von international agierenden Unternehmen und Konzernen besteht das interne Netzwerk typischerweise aus einer unübersichtlichen Anzahl an Teilnetzwerken und Systemen. Dies liegt in den meisten Fällen daran, daß Computernetzwerke in Konzernen im Laufe von Jahren durch Unternehmenszukäufe und strukturelle Reorganisationen „gewachsen“ sind und die Produktionsfähigkeit zunächst meist eine höhere Priorität genießt als die Sicherheit des gesamten Netzwerkes.

Weiterhin unterlassen es Firmen teilweise absichtlich, verfügbare Sicherheits-Updates zu installieren, da sie vom Hersteller ihrer Software nur für „zertifizierte Plattformen“ Support in Anspruch nehmen können. Werden also in solchen Fällen nach bekanntgewordenen Sicherheitslücken Updates eingespielt, verlieren die Unternehmen die technische Unterstützung ihres Softwareanbieters. Um dennoch Maßnahmen gegen die bekannte Schwachstelle zu ergreifen, wird üblicherweise die Firewall mit einem Filter versehen. Gerade diese Firmen benötigen dann Exploits, um zu testen, ob ihr Filter tatsächlich funktioniert.

Neben Exploits und weiteren sogenannten Angriffswerkzeugen existieren zusätzlich zahlreiche Frameworks, also „Bausätze“ oder Grundlagenmodule, um sehr einfache Angriffswerkzeuge herzustellen, die auf die individuellen Schwachstellen und Risiken in Unternehmensnetzwerken abgestimmt sind. Diese Frameworks können und werden gleichermaßen sowohl von boshaften Angreifern als auch von Beratungsunternehmen und internen IT-Sicherheitsabteilungen verwendet.

---

[12] Ein „0-Day“-Exploit bezeichnet ein verwirklichtes Verfahren zur Ausnutzung bislang unbekannter Sicherheitslücken in verbreiteter Software. Ein Exploit (engl. für Ausnutzung) ist allgemein ein entwickeltes und programmatisch umgesetztes Verfahren, um eine Schwachstelle eines Dienstes oder in einer Software, zum Beispiel in einem Betriebssystem, zum Vorteil des Angreifers auszunutzen. Angreifer können mittels des Exploits beispielsweise ein System unter die eigene Kontrolle bringen, ohne daß dies vom Eigentümer oder Nutzer des Systems bemerkt würde. Sie dienen also als Demonstration und mithin als Beweis, daß ein Angriff in einer bestimmten Form möglich ist und zum Erfolg führt. Die meisten Exploits sind allgemein öffentlich zugänglich. Beispielhaft sei hier der milw0rm-Exploit angeführt:

```
<script>document.location='ircs://blabla@3.3.3.3" --command "shell calc"'</script>
```

Er beschreibt konkret, wie man eine Sicherheitslücke ausnutzt, und kann direkt zum Testen auf Verwundbarkeit am eigenen Rechner sowie zum Angriff genutzt werden. Siehe http://milw0rm.com/exploits/5795 vom 13. Juli 2008.

2.4 Beispiel Webbrowser

Zu den momentan meistverwendeten Programmen gehören sogenannte Webbrowser. Diese Programme ermöglichen es dem Benutzer, Webseiten im World Wide Web (WWW) zu betrachten und mit ihnen zu interagieren. Der Markt für Webbrowser wird von wenigen Produkten beherrscht: Mozilla Firefox, Microsoft Internet Explorer und Apple Safari. Angebote im WWW entwickeln sich technisch in einer bis dato ungeahnten Geschwindigkeit weiter, was wiederum die Hersteller der Webbrowser dazu zwingt, immer neue Technologien in ihre Produkte zu integrieren, um sie dem Benutzer zugänglich zu machen. Prinzipiell gibt es hierbei keine Korrelation zwischen dem verwendeten Webbrowser und der Webseite, welche verwendet werden soll, jede Webseite sollte also auch mit jedem Webbrowser funktionieren.

Die weite Verbreitung von Webbrowsern macht diese natürlich auch zu einem sehr lohnenden Ziel für Angriffe. Die Hersteller von Webbrowsern versuchen, durch technische Regelwerke in ihren Produkten zu verhindern, daß Anwender Opfer solcher Angriffe werden, wenn sie Webseiten mit bösartigem Inhalt aufsuchen. Aufgrund der Komplexität der Interaktionen eines Webbrowsers mit dem WWW kann dies aber nicht in allen Fällen gelingen. Trifft der Webbrowser in einer bestimmten Konstellation von Ereignissen die falsche Entscheidung, ist dies ein Fehlverhalten, welches von einem Angreifer ausgenutzt werden kann.

Da alle Webbrowser prinzipiell die gleichen Funktionen zu erfüllen haben, treten solche Fehler auch häufig bei Produkten verschiedener Hersteller gleichermaßen auf. Dies wird nur deutlich, nachdem eine Schadsoftware oder ein Nachweis eines solchen Fehlers entdeckt und publiziert wurde, denn nur so können Programmierer und Anwender anderer Webbrowser die Anfälligkeit ihrer eigenen verwendeten Produktes gegen dieselbe Fehlentscheidung überprüfen. In der Vergangenheit war es häufig der Fall, daß ein Fehler in einem Webbrowser-Produkt analog bei den anderen Herstellern aufgetreten ist. Aus diesem Grund tauschen die Hersteller täglich Informationen über neu entdeckte Fehlverhalten in ihren Produkten aus.

Die vorangegangenen Beispiele machen deutlich, daß sowohl die eigene Entwicklung als auch der Besitz sowie der Austausch von Wissen über Schadsoftware notwendig sind, um eine Fehleranalyse sinnvoll betreiben zu können. Die tatsächliche Wirkung eines Fehlers in einer Software ist nur anhand solcher Analysen konkret prüfbar.

2.5 Schließen von Sicherheitslücken erfordert Angriffscode

Analysiert man auf die Gründe, die ursprünglich dazu geführt haben, daß Hacker anfingen, gefundenen Exploits zu veröffentlichen, so geschah dies oft aufgrund der Tatsache, daß Softwarehersteller die Existenz eines Sicherheitsproblems geleugnet haben. Hacker nahmen dieses vehemente Leugnen und Herunterspielen von Sicherheitsproblemen zum Anlaß, als Beweis ihre Exploits zu veröffentlichten. Erst damit wurde der Druck auf die Hersteller der betroffenen Software groß genug, den Fehler ihren Anwendern einzugestehen und zu beheben. In Zukunft wird durch die neue Gesetzeslage das Risiko des Öffentlichmachens für den „Finder“ erheblich vergrößert.

Softwarehersteller leugnen Sicherheitslücken dabei oftmals aufgrund wirtschaftlichen Drucks. Es ist etwa für einen großen Anbieter wie Microsoft

finanziell vorteilhaft, Schwachstellen durch eigene Forschung zu finden und den Benutzern mit dem nächsten „Service Pack“ die jeweilige Korrektur anzubieten. Diese „Service Packs“ werden nur in großen Zeitabständen von mehreren Monaten oder Jahren veröffentlicht. Microsoft kostet es dagegen deutlich mehr, auf eine von außen an die Firma herangetragene kritische Sicherheitslücke schnell reagieren zu müssen, da hier sofortiges Testen und eine schnelle Abhilfe geboten sind. Noch billiger ist es kurzfristig für ein Unternehmen sogar, auf gefundene Fehler gar nicht zu reagieren. Es gibt also einen starken wirtschaftlichen Anreiz für Softwarehersteller, Schwachstellen zu leugnen. Nur die Veröffentlichung eines Exploits liefert daher ein wirtschaftlichen Grund, angemessen zu reagieren.

Nicht erst durch die sich in jüngster Zeit häufenden Fälle von bekannt gewordenen Sicherheitslücken bei Unternehmen und Behörden wird deutlich, wie wichtig die Funktion solcher Veröffentlichungen ist, da kritische Infrastruktur heute in weiten Teilen auf Computertechnik basiert.

Exploits sind ein wichtiger Bestandteil zur Selbstregulierung des IT-Marktes. Wenn sich ehrenamtliche Hacker, aber auch mittelständische IT-Unternehmen durch die neue Gesetzgebung darin behindert sehen, notwendige Software zu entwickeln und verwenden sowie gefundene Schwachstellen zu veröffentlichen, verschließen sie gleichsam gezwungenermaßen die Augen vor einem größer werdenden Problem. Entsprechend sinkt der Druck auf Hersteller und Anbieter, ihre Softwareprodukte zu sichern und zu verbessern. Denn ohne einen beweisbaren Exploit ist es nur schwer nachweisbar, daß eine Software ein Problem beinhaltet. Ohne diesen Nachweis kann sich ein Hersteller also weigern, das Sicherheitsproblem anzuerkennen und in der Folge abzustellen.

Ein häufig vorgebrachtes Argument für die gesetzliche Beschränkung von „Computereinbruchswerkzeugen“ ist es, daß die Erstellung solcher Software unnötig sei, da es doch ausreiche, eine gefundene Sicherheitslücke abstrakt zu beschreiben. Der Hersteller würde das Problem dann schnell beheben, bevor ein tatsächliches Angriffswerkzeug gebaut und verbreitet wurde.

Diese Ansicht geht indes an der Realität der tatsächlichen IT-Sicherheitsforschung vollends vorbei. In der Praxis werden Sicherheitslücken sowohl von den Herstellern als auch von den verantwortlichen IT-Managern in den Unternehmen nach einem Kriterienkatalog priorisiert. Diese Priorisierung bestimmt, welche Schwachstellen bevorzugt bearbeitet werden, für welche Sicherheitslücken eine Softwareanpassung (sogenannter Patch) erstellt und zum Einsatz gebracht wird.

Angesichts der großen Zahl an gefundenen Sicherheitslücken und der potentiellen unerwünschten Nebenwirkungen, die durch die Patches entstehen können, wird üblicherweise eine Rangliste anhand von bestimmten Kriterien erstellt, die spezifisch für die Situation des jeweiligen Unternehmens sind. Beispielsweise wird hier berücksichtigt, wie verbreitet die von der Sicherheitslücke betroffene Software im Unternehmen oder im gesamten Markt eingesetzt wird, welche potentiellen Auswirkungen ein erfolgreicher Angriff haben könnte und wie wahrscheinlich ein Angriff gegen diese Schwachstellen ist.

Eines der wichtigsten Kriterien für das schnelle Einspielen eines Patches ist für alle Unternehmen jedoch das Vorhandensein eines beispielhaften Angriffswerkzeugs, das nachweist, daß die Lücke tatsächlich existiert und

ausgenutzt werden kann, mithin eben nicht nur theoretischer Natur ist. Sobald das Ausnutzen der Schwachstelle für einen Angriff vom Systembetreuer selbst nachvollzogen werden kann, ist ihm unmittelbar klar, daß gehandelt werden muß.

Eine ähnliche Priorisierung findet bei den Herstellern bzw. Entwicklern von Software statt. Gerade bei weitverbreiteten Komponenten gibt es häufig Fehlalarme. Ein Fehlalarm ist dadurch gekennzeichnet, daß etwa Sicherheitslücken berichtet werden, diese sich aber bei näherer Betrachtung als nicht ausnutzbar herausstellen oder anderweitig irrelevant sind. Das Vorhandensein eines sogenannten „Proof of Concept“[13] verdeutlicht dem Hersteller jedoch, daß es sich bei der gefundenen Sicherheitslücke nicht um einen Fehlalarm handelt und daher eine hohe Priorität bei der Bearbeitung angemessen ist. Das Vorhandensein eines Werkzeugs, mit der sich die Schwachstelle ausnutzen läßt, beschleunigt somit die Anstrengungen zum Schließen der Lücke. Hersteller bieten also üblicherweise erst dann Abwehrmaßnahmen an, wenn es bereits einen Exploit gibt.

Mittlerweile wird ein nicht unerheblicher Teil von schwerwiegenden Sicherheitslücken, die von individuellen Sicherheitsforschern bzw. kleinen Unternehmen gefunden werden, von den Herstellern bzw. durch sie beauftragte spezialisierte IT-Unternehmen aufgekauft, um einer Weiterverbreitung vorzubeugen und gleichzeitig das finanzielle Budget eigener Sicherheitsforschung zu senken. Auch hier ist das Vorhandensein eines tatsächlich funktionsfähigen Werkzeugs zum Ausnutzen der jeweiligen Sicherheitslücke praktisch Bedingung für einen erfolgreichen Verkauf des Wissens um die Schwachstelle. Ohne „Proof of Concept“ findet in der Praxis ein Ankauf entweder gar nicht oder nur zu einem erheblich reduzierten Preis statt.

Die Mechanismen des IT-Sicherheitsmarktes machen also aus rein praktischen Gründen das Erstellen von Software, die eine gefundene Sicherheitslücke ausnutzt, notwendig. Eine andere Vorgehensweise ist in der Mehrzahl der Fälle schon aus technischen Gründen kaum möglich, da eine rein theoretische Beschreibung der Schwachstelle zu einer Vielzahl von Fehlalarmen führt, die nicht mehr ökonomisch zu bearbeiten sind. Die Hersteller von Softwareprodukten und anderen informationstechnischen Systemen sind daher darauf angewiesen, daß gefundene Sicherheitslücken mittels eines praktischen Nachweises dokumentiert werden und damit hinsichtlich der tatsächlichen Anwendbarkeit bewiesen sind.

Deutsche Sicherheitsforscher können durch die derzeitige Fassung des § 202c StGB diesen auf dem IT-Sicherheitsmarkt etablierten Prozeduren nur unter großer Rechtsunsicherheit folgen. Der Verkauf einer Sicherheitslücke mit dazugehörigem „Proof of Concept“ beispielsweise an eine spezialisierte Beratungsfirma oder den Hersteller der betroffenen Software ist im Zweifel bereits illegal. Nach dem Wortlaut des Paragraphen ist ein solches Vorgehen sogar in jedem Fall rechtswidrig.

2.6 Besitz von Schadsoftware notwendig für Ausbildung

Forschung und Wissen im Bereich der IT-Sicherheit wird keineswegs ausreichend an den Universitäten gelehrt und auch nicht während einer Berufsausbildung vermittelt. Diejenigen Fachkräfte, die im Bereich der IT-Si-

[13] Ein „Proof of Concept“ ist der praktische Nachweis der Funktionsfähigkeit eines Angriffes.

cherheit erfolgreich arbeiten und einen Großteil des Wissens besitzen, der für solche Aufgaben notwendig ist, haben in der Regel über viele Jahre hinweg ein persönliches Interesse an dieser Thematik entwickelt und dies unabhängig von der Ausbildung weiterentwickelt und gepflegt.

Hierzu gehört selbstverständlich auch das eigenständige Experimentieren mit selbstgeschriebenen Programmen und öffentlich bekannten Schadprogrammen sowie mit entsprechenden Werkzeugen, um diese gegebenenfalls zu neutralisieren oder einzuschränken. Diese Werkzeuge, die für eine Absicherung von Netzwerken dienen und genutzt werden, um die aktuell bestehende Konfiguration einzelner Systeme und Komponenten aus der Sicherheitsperspektive zu betrachten, fallen heute in die bestehende rechtliche Grauzone des § 202c StGB.

Angehende und bereits im Beruf stehende Informatiker sowie all diejenigen, die sich grundsätzlich für die IT-Sicherheit interessieren und nach Abschluß des Studiums oder einer Ausbildung in dieser Branche tätig werden wollen, müssen sich somit mit einer rechtlich unsicheren neuen Situation auseinandersetzen.

Für die tiefgehende Beschäftigung mit Fragen der IT-Sicherheit ist es unbedingt notwendig, sich auch mit diversen Techniken auseinanderzusetzen, die in Verbindung mit krimineller Energie tatsächlich einen großen Schaden hervorbringen könnten. Das Training und die Aufarbeitung dieses Wissens ist darüber hinaus tatsächlich oft nur bei denjenigen möglich, die sich auch in ihrer Freizeit und häufig spielerisch mit diesen Techniken und Werkzeugen befassen. Allein durch eine universitäre Ausbildung kann kein Unternehmen von einem Studienabgänger erwarten, die notwendigen Informationen und Erfahrungen für die wichtigen Positionen in den IT-Sicherheitsabteilungen zu erlangen. Gute Sicherheitsexperten werden eben nicht „im Reinraum gezüchtet“, sondern erlernen über viele Jahre hinweg selbständig ihr Wissen durch kontinuierliches Ausprobieren, aber auch den Austausch mit Gleichgesinnten.

Der private Besitz sogenannter Schadsoftware ist für eine Beschäftigung und Wissenserweiterung notwendig. Universitäten und Ausbildungsbetriebe sind in der Regel lediglich in der Lage, während der Ausbildung ein Breitenwissen im Bereich der Informatik zu vermitteln. Zwar werden im Rahmen eines Informatikstudiums auch IT-Sicherheitsaspekte thematisiert, dies ist jedoch keinesfalls in dem Umfang möglich, wie es von Unternehmen im IT-Beratungssektor oder von Konzernen mit erhöhtem Schutzbedarf erwartet wird. Eine Spezialisierung im Anschluß an eine Ausbildung ist somit notwendig, um die Ansprüche potentieller Auftraggeber und Arbeitgeber erfüllen zu können.

Im Gebiet der IT-Sicherheit sind die Vorgehensweisen hinsichtlich der Entwicklung neuer Techniken und Verfahren erfahrungsgemäß grundlegend anders als in anderen Fachgebieten. Die Analyse und Entwicklung neuer Techniken, um Schwachstellen auszunutzen, schreitet in außerordentlich hohem Tempo fort. Dies charakterisiert die Forschung im Bereich Informatik und informationstechnischer Systeme in besonderer Weise.

Die Entwicklung neuer Angriffstechniken geht stets einher mit den jeweiligen Verfahren und Anregungen, wie sich Anwender gegen neue Klassen von Schwachstellen schützen können. Ist ein Forscher durch eine rechtlich unklare Situation jedoch eingeschränkt, auch privat seine Forschungsergebnisse öffentlich zu thematisieren und zu diskutieren, werden solche

Ergebnisse einer breiten Öffentlichkeit nicht mehr zugänglich sein. Diese Öffentlichkeit schließt hier selbstverständlich auch Unternehmen ein, die selbst von den Problemen betroffen sein könnten, wie zum Beispiel Software- und Betriebssystemhersteller, Anti-Viren-Hersteller etc.

Die Entwicklung oder Identifizierung neuer Schwachstellen- und Fehlerklassen setzt eine umfangreiche Forschung in einem bestimmten Gebiet voraus. Im Tagesgeschäft eines Unternehmens, welches entweder beratend tätig ist oder eigene IT-Sicherheitsabteilungen unterhält, ist es nahezu unmöglich, eine solch tiefgehende Forschung zu finanzieren. All diese Unternehmen sind zum großen Teil auf das Engagement und persönliche Interesse der IT-Forscher angewiesen, die in ihrer Freizeit weiter an neuen Techniken und Forschungen arbeiten.

Ebenso sind solche Unternehmen darauf angewiesen, daß insbesondere noch unerfahrene Mitarbeiter Teile ihrer Sicherheitsforschung und Weiterbildung außerhalb des Tagesgeschäfts des Unternehmens durchführen. Besonders kleine bis mittelständige Unternehmen können nur auf diese Weise junge und unerfahrene Mitarbeiter anstellen und finanzieren, da eine vollständige Finanzierung der Forschungsarbeit und Weiterbildung innerhalb des Betriebes keinen direkten Gewinn für das Unternehmen bringt und daher auch bei nachweislichem Bedarf nur schwer durchsetzbar ist.

Eine Person, die entweder als Einsteiger oder auch als professioneller IT-Sicherheitsberater tätig ist, muß also auch in seinem privaten Umfeld mit sogenannten Hackerwerkzeugen und/oder Schadsoftware experimentieren und sie selbst entwickeln dürfen. Hierbei sollte es unter keinen Umständen eine Rolle spielen, ob die Person tatsächlich beruflich im IT-Sicherheitsbereich tätig ist oder nicht. Ausschließlich privates Engagement in der Forschung und beim Erlernen von Analyse- und Abwehrtechniken kann es einem IT-Sicherheitsspezialisten erlauben, sich für Anstellungen in dieser Branche zu qualifizieren.

Die Unsicherheit und Angst vor einer Strafverfolgung ist somit insbesondere für diese Gruppe potentiellen Nachwuchses besonders hoch, da sie die Rechtfertigung des Besitzes und der Entwicklung von Schadsoftware (noch) nicht auf eine berufliche Verwendung stützen kann. Sollten diese Personen – zufällig oder nicht – in das Visier von Ermittlern geraten, könnten Zufallsfunde wie Schadsoftware oder vermeintliche Hackerwerkzeuge der Person nachteilig ausgelegt werden, obwohl keine strafbare Handlungen durchgeführt wurden.

2.7 Forschung nach neuen Fehlerklassen

Schwachstellen in Softwareprodukten, die von Angreifern ausnutzbar sind, um zum Beispiel schadhaften Code zur Ausführung zu bringen, können allgemein als Softwarefehler betrachtet werden. Solche Fehler sind zunächst undefinierte Zustände, in die eine Software gelangen kann, wenn zuvor definierte Schnittstellen nicht korrekt genutzt werden oder Funktionalitäten bereitgestellter Module oder anderer Programme bzw. deren Nebeneffekte nicht hinreichend bekannt sind.

Die Abhängigkeit der Softwareentwickler von anderen Entwicklungswerkzeugen, wie zum Beispiel Programmen, welche den Quelltext in ein maschinenlesbares Format übersetzen, ist groß. Existieren Fehler in diesen Entwicklungswerkzeugen, kann dies unüberschaubare Auswirkungen auf

ein finales Softwareprodukt mit sich bringen. Somit muß ein Softwareprodukt einem lebenslangen Zyklus der Qualitätssicherung unterworfen werden, um langfristig und regelmäßig auf Fehler und Fehlerklassen reagieren zu können.

Die Frage, ob ein einmal identifizierter Fehler einer Software, der beispielsweise zu einem undefinierten Zustand führt, ein Sicherheitsrisiko darstellt, kann grundsätzlich nicht beantwortet werden, sofern nicht ein Forscher konkret das Gegenteil beweist. Die Forschung bezüglich potentieller neuer Fehlerklassen, die aus der Sicherheitsperspektive relevant sein könnten, ist insofern nur noch eingeschränkt möglich, da Forscher Gefahr laufen, kriminalisiert zu werden, sobald sie öffentlich über solche potentiellen Schwachstellen diskutieren und eigene Ergebnisse und Werkzeuge verbreiten.

Eine öffentliche Diskussion ist jedoch notwendig für solch komplexe Forschungen, da diese in der Regel sehr aufwendig sind und ein Austausch zwischen Experten mit unterschiedlichen Schwerpunkten unabdingbar ist. Findet eine solche öffentliche Diskussion zwischen verschiedenen Forschern nicht statt, ist die Gefahr hoch, daß ganze Klassen von (neuen) Schwachstellen unerkannt bleiben. Kann die Diskussion und der Austausch von Forschungsergebnissen uneingeschränkt stattfinden, besteht die Möglichkeit, die Öffentlichkeit und die Softwarehersteller für eine neue Fehlerklasse zu sensibilisieren, sodaß bestimmte Fehler bei der Entwicklung von Software berücksichtigt werden. Nur wenn eine solche Sensibilisierung stattfindet, kann langfristig von einer immer sicherer werdenden Softwareentwicklung gesprochen werden, von der in erster Linie die Anwender profitieren.

Softwarehersteller, die besonders hohe Anforderungen an ihr Softwareprodukt haben, weil es zum Beispiel in der Raumfahrt oder Landesverteidigung verwendet wird, sind durch die Einführung des § 202c StGB gegebenenfalls bei der Definition ihrer Softwareentwicklungsprozesse stark eingeschränkt. Ein solcher Prozeß, auch Softwareentwicklungsmodell genannt, definiert den Lebens- und Entwicklungszyklus einer zu programmierenden Software. Bei besonders hohem Schutzbedarf kann ein solcher Prozeß auch die gezielte Suche nach potentiellen neuen Klassen von Schwachstellen beinhalten.

Diese Art der Forschung bewegt sich auch hier nach der neuen Gesetzgebung in einer rechtlichen Grauzone, da zunächst ausschließlich nach Verfahren geforscht wird, Fehler für bösartige Zwecke auszunutzen. Ist ein Fehler einmal identifiziert, kann ein solcher Softwareentwicklungsprozeß vorschreiben, mittels einer Breitensuche im gesamten Softwareprodukt und den verwendeten Komponenten oder Modulen von Drittanbietern nach Fehlern dieser neuen Klasse zu suchen. Solch ein Prozeß und die hiermit verbundenen Forschungen bewegen sich durch den § 202c StGB auf einer unsicheren rechtlichen Grundlage und können je nach Auslegung zum Nachteil der involvierten Personen und Unternehmen ausgelegt werden.

2.8 Das Recht auf digitalen Selbstschutz

Das Bundesverfassungsgericht hat in seinem Urteil zur Online-Durchsuchung festgestellt, daß vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme das Interesse des Nutzers geschützt ist, daß „die von einem vom Schutzbereich erfassten

informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben."[14] Das Recht und nicht selten auch die gesetzliche Pflicht zum aktiven Schutz der eigenen Daten, wie sie im Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme niedergelegt sind, läßt sich praktisch nur durch die aktive und fortgesetzte Überprüfung der eigenen Systemsicherheit gewährleisten. Von besonderer Bedeutung ist dieses Grundrecht von dem Hintergrund, daß die Anzahl und technische Qualität von Angriffen gegen IT-Systeme, insbesondere auch aus dem außereuropäischen Ausland, weltweit fortlaufend zunehmen.

Als Benutzer eines informationstechnischen Systems allein darauf zu vertrauen, daß Täter durch potentielle Strafverfolgung abgeschreckt werden, ist illusorisch. Angesichts der zunehmenden Verwendung von Netzwerkangriffen für Zwecke der Industriespionage[15] und für massenweisen Identitätsdiebstahl sind Bürger und Unternehmen zwingend darauf angewiesen, selbst effektive Sicherheitsmaßnahmen für ihre Computer anzuwenden und deren Effektivität zu überprüfen.

Im Bereich der IT-Sicherheit muß daher neben der Verwendung von Verschlüsselungsverfahren, Firewalls, Anti-Viren-Systemen und ähnlichen Schutztechniken auch immer eine aktive Überprüfung der tatsächlich vorhandenen Systemsicherheit erfolgen. Das Recht, die eigenen Daten vor unbefugtem Zugriff zu bewahren, muß daher auch das Recht einschließen, sein eigenes IT-System testhalber anzugreifen, um Schwachstellen aufzudecken. Sofern ein Computerbenutzer nicht selbst in der Lage ist, sein System auf Angreifbarkeit zu überprüfen, muß er selbstverständlich auch Dienstleister beauftragen dürfen.

Der vom Bundesverfassungsgericht geforderte besondere Schutz der Integrität informationstechnischer Systeme wird durch den § 202c StGB inhaltlich konterkariert, da der Paragraph diesen Schutz der Integrität für den Benutzer des Systems erheblich erschwert oder unmöglich macht.

---

[14] BVerfG, 1 BvR 370/07 vom 27. Februar 2008, Rd.-Nr. 204.

[15] Vgl. Bundesministerium des Innern: Verfassungsschutzbericht 2007, S. 270.

3 Geeignetheit des § 202c StGB

Tatsächliche häufig vorkommende kriminelle Aktivitäten werden durch die Änderungen im StGB nicht tangiert: Kriminelle werden trotz der Gesetzesänderung auch in Zukunft kein erhöhtes Risiko der Strafverfolgung erfahren.

Für Kriminelle, die Computerangriffe häufig als Lebensunterhalt betreiben, ist die zusätzliche Strafnorm des § 202c irrelevant, sie wollen prinzipiell eine Entdeckung vermeiden und agieren daher in der Regel konspirativ und über verschiedenste Rechner außerhalb der EU. Diese Personen haben meistens mehr zu verbergen als nur eine Sammlung an Angriffswerkzeugen und agieren daher entsprechend. Kriminelle Aktivitäten im Internet werden erfahrungsgemäß in Ländern in die Wege geleitet, in denen der Täter kaum Strafverfolgung fürchten muß.

Angriffswerkzeuge, die für die komplexeren und lukrativsten Formen der Computerkriminalität, wie etwa Phishing, verwendet werden, sind in der Regel individuell zusammengestellt. Dies erfordert eine gewisse Expertise auf Seiten der Kriminellen. Diese Personen sind daher nur in reduziertem Maße auf Software und Werkzeuge aus allgemein zugänglichen Quellen angewiesen.

Die Verfügbarkeit von potentieller Schadsoftware ist durch den § 202c StGB in keiner für Kriminelle signifikanten Weise eingeschränkt worden. Die Mehrzahl der Angriffe auf deutsche IT-Systeme findet ohnehin aus dem Ausland statt, selbst eine leichte Erhöhung der Zugangsschwelle im deutschsprachigen Raum ist also irrelevant. Durch die nach der Gesetzänderung zu verzeichnende Zurückhaltung seriöser deutscher Informationsquellen (siehe Kapitel 4.2) lassen sich die in der Regel mit hoher krimineller Energie und Beharrlichkeit agierenden Täter nicht abschrecken. Im Gegenteil: Durch das Abdrängen in die Grauzonen des Netzes wird erst der Kontakt zu Gleichgesinnten erzwungen, der dann im Zweifel zu erweiterten kriminellen Aktivitäten führt.

Durch die rechtliche Unsicherheit für Sicherheitsforscher und Unternehmen im Umgang mit potentieller Schadsoftware ergibt sich zudem ein fallendes Sicherheitsniveau deutscher IT-Systeme. Da Selbsttests mit Angriffswerkzeugen unterbleiben oder nur eingeschränkt durchgeführt werden, bleiben die Systeme für diese Werkzeuge angreifbar, sodaß Kriminelle auch auf einem niedrigeren technischen Niveau zum Erfolg kommen können. Die entsprechende Software dafür kann in einfacher Weise aus ausländischen Quellen beschafft werden.

Bei der Vorbereitung einer Computerstraftat ist die Beschaffung geeigneter Software für Kriminelle weitgehend unproblematisch, da im Internet über offene Quellen oder über nicht-öffentliche Zugangswege praktisch alle denkbaren Angriffswerkzeuge unterschiedlichster Komplexität verfügbar sind. Im nicht-öffentlichen Bereich findet zusätzlich ein reger Austausch über Foren und Dateitausch-Netzwerke statt, die nicht oder nur sehr aufwendig zu überwachen sind. Eine Offenlegung aller Zugangswege zu potentieller Schadsoftware wäre auch nicht im Wege einer umfassenden und vollständigen Internet-Zensur denkbar. Aufgrund der Vielzahl von Zugangswegen und nicht einsehbaren verschlüsselten Kommunikationsprotokollen würde selbst eine so drastische Maßnahme keinen signifikanten Erfolg versprechen. Das für auch nur einen teilweisen Erfolg einer solchen Maßnahme notwendige Ausmaß an flächendeckender Überwachung von

Kommunikationsinhalten – deren Erfolg zudem bezweifelt werden dürfte – wäre ungeeignet und damit unverhältnismäßig.

Wie bereits dargelegt, ist in den meisten Fällen nicht einmal der Einsatz besonderer, schwer verfügbarer Werkzeuge nötig. In der Praxis zeigt sich, daß Angriffe in der Regel mit einfachsten Mitteln erfolgreich durchgeführt werden können.

Eine aktuelle Studie, die auf der Analyse von über 500 entdeckten Computereinbrüchen beruht, belegt, daß fast drei Viertel aller Angriffe auf einem technisch eher niedrigen Niveau stattfinden.[16] Es werden Standardwerkzeuge verwendet, die in den meisten modernen Betriebssystemen für alltägliche legale Zwecke vorhanden sind oder die sich mit nur geringem Aufwand an tausenden Stellen im Internet herunterladen lassen. Ein nicht geringer Teil der Angriffe wird einfach über einen normalen Webbrowser durchgeführt, in dem z. B. URLs erraten werden oder mangelhafte Konfigurationen auf dem Zielsystem ausgenutzt werden. Inkompetenz oder Nachlässigkeit auf Seiten des Systembetreibers ist mithin das weitaus größte Sicherheitsrisiko. Kriminelle haben dies längst erkannt und wählen ihre Ziele dementsprechend aus.

Nur in der Minderheit der Fälle werden spezialisierte Werkzeuge benutzt, deren Benutzung und Anpassung eine gewisse Expertise erforderte. Die Kriminellen, die sich auf diese Art von Angriffen spezialisiert haben, haben keinerlei Beschaffungsbarriere, um sich die notwendigen Werkzeuge im Internet zu beschaffen. Gegebenenfalls wird die benötigte Software selbst erstellt. Wie schon ausgeführt, ist für die Erstellung eines Angriffswerkzeugs nur ein normaler Computer erforderlich.

Erfahrungsgemäß wird für den Angriff der Weg des geringsten Widerstands gewählt. Das am schlechtesten gesicherte System, bei dem sich mit dem geringstmöglichen Aufwand ein Erfolg erzielen läßt, wird also angegriffen. Dies ist vergleichbar mit dem in der Alltagskriminalität beobachteten Muster, daß etwa ein Wohnungseinbruch in der am schlechtesten gesicherten Wohnung eines Hauses erfolgt. Der Einbrecher wird hier auch nicht mit aufwendigen Schloßöffnungswerkzeugen vorgehen, sondern probieren, wo er mit einfachen Werkzeugen zum Ziel kommt.

Bedingt durch die bereits erläuterte nicht eindeutige Zweckbestimmtheit eines Software-Werkzeugs ist die Einschränkung der Verbreitung unmöglich. Wenn sich die Strafnorm an den realen Fallstrukturen orientieren würde, müßten Webbrowser und die mit Standardbetriebssystemen ausgelieferten Werkzeuge verboten werden, da mit diesen die Mehrzahl der Angriffe erfolgt. Diese Werkzeuge werden keineswegs mit einem Schädigungsvorsatz vertrieben oder veröffentlicht. Wie jedoch ein Anwender die Software verwendet und ob er nur lautere Ziele damit verfolgt, liegt nicht in der Hand der Softwarehersteller. Dennoch machen sie sich nach der neuen Gesetzeslage unter Umständen strafbar. Zumindest jedoch entsteht für die Entwickler und Softwarehersteller eine Unsicherheit, wann die Grenzen zur Strafbarkeit überschritten ist.

International wird der Versuch, eine künstliche Grenze zwischen „guter“ und „böser“ Software zu ziehen, mit großer Verwunderung betrachtet. Wie

---

[16] Verizon Business Risk Team: Data Breach Investigations Report, 2008, http://www.verizonbusiness.com/resources/security/databreachreport.pdf vom 12. Juli 2008.

bereits dargelegt, ist die Verfügbarkeit von potentiell schädlichen Software-Werkzeugen unabdingbar für wirksame Sicherheitsanalysen. Daher gibt es kaum internationale Sympathie für Versuche, die Verbreitung dieser Software derart weitgehend zu limitieren oder einzustellen. Auf lange Sicht ist absehbar, daß sich Deutschland durch die neue Gesetzeslage zu einem Ziel ausländischer Angriffe entwickeln wird, da die Folgen der Fehlentscheidung des Gesetzgebers Kriminellen, etwa im Bereich Wirtschaftsspionage, nicht entgehen werden.

Im Bereich der Viren und Trojaner müssen potentielle Kriminelle nicht einmal zur aktiven Beschaffung oder zur eigenen Programmierung schreiten. Es genügt, eine Handvoll E-Mailadressen zu besitzen und die eingehenden E-Mails einer sorgfältigen Analyse zu unterziehen. Die Verbreitung unverlangter Werbe-E-Mail („Spam“) mit Schadsoftware ist so groß, daß in der Regel innerhalb weniger Tage eine beachtliche Kollektion an Schadsoftware zusammenkommt, die dann den eigenen Bedürfnissen angepaßt werden kann. Dieses Vorgehen wird seit vielen Jahren beobachtet. Neue Viren und Trojaner sind sehr häufig bereits bekannte Programme, die bei Kriminellen via unverlangt eingesandter E-Mail „angespült“ wurden und dann direkt im Binärcode leicht modifiziert und für eigene Zwecke weiterverwendet werden.

Dieses Vorgehen kann im übrigen auch im Geheimdienstbereich beobachtet werden. Werkzeuge für die sogenannten Online-Durchsuchungen beruhen teilweise auf Modifikationen von im Internet bereits kursierender Schadsoftware. Dabei werden in der Regel kaum mehr als die Adresse und die Zugangskennung des Steuercomputers geändert, bei dem die Schadsoftware die gewonnenen Daten vom infizierten Computer abliefert und neue Befehle entgegennimmt. Der Betroffene wird bei einer Entdeckung annehmen, daß es sich um „normale“ Internetkriminalität handelt, und daher keinen geheimdienstlichen Hintergrund vermuten. Bei entsprechend geschickt verschleierter Wahl des Steuerrechners ist im Zweifel nicht einmal bei detaillierter Analyse der Schadsoftware eine Unterscheidung zwischen geheimdienstlichem Handeln und normaler Internetkriminalität möglich.

4 Auswirkungen der Strafrechtsänderung

So wie die Autoindustrie ihre Fahrzeuge mit Crashtests testet, prüfen Experten in der Computerbranche die Systemsicherheit durch den kontrollierten Einsatz von Angriffsprogrammen.

Durch die neue Gesetzgebung sind zunächst vor allem Unklarheiten für Auftraggeber der IT-Sicherheitsunternehmen entstanden. Als typische Angaben im Bereich solcher Unternehmen seien hier beispielhaft die Aussagen des Teilhabers und Geschäftsführers der Code Blau GmbH[17], Felix von Leitner, angeführt.

> „Aus Sicht unserer Branche ist das ‚Hackertoolverbot' ein Desaster. Praktisch alle Kunden dieses Jahr haben vor Aufträgen besorgt nachgefragt, ob wir denn angesichts des ‚Hackertoolverbots' überhaupt noch ordentlich unsere Arbeit machen können. Wir konnten die Kunden beruhigen – die, die nachgefragt haben. Wir gehen aber davon aus, daß es hier eine Dunkelziffer an potentiellen Kunden gibt, die uns gar nicht erst angesprochen haben. Der Markt ist stark verunsichert, viele Firmen glauben, sie könnten sich juristisch angreifbar machen, wenn sie eine Sicherheitsfirma wie uns beauftragen, die dann womöglich in einer juristischen Grauzone agieren muß, und wagen daher nicht, ihre Sicherheitsprobleme offensiv anzugehen.
>
> Unter dem Strich ergibt sich hier eine deutliche Verschlechterung der Sicherheitsstandards in Deutschland. Gerade in Zeiten der Produktpiraterie und Industriespionage (die China-Trojaner seien hier beispielhaft erwähnt, die es ja sogar in diverse Ministerien geschafft haben) kann sich der Wirtschaftsstandort Deutschland das aus unserer Sicht nicht leisten.
>
> Aber auch unsere Arbeit wird durch das ‚Hackertoolverbot' ganz konkret beeinträchtigt. Wir hatten kürzlich einen Kunden im Ausland, eine Bank. Diese Bank betreibt einen Online-Banking-Webserver und wollte von uns wissen, ob der angreifbar ist. Auf dem Webserver lief eine alte Programmversion mit bekannten Sicherheitsproblemen. Da wir im Ausland operiert haben, konnten wir einen Exploit aus dem Internet holen und vor Ort gegen den Webserver anwenden und so nicht nur demonstrieren, daß der Webserver unsicher war, sondern sogar Spuren von früheren Einbrüchen auf dem Webserver finden.
>
> Wäre dieser Kunde eine inländische Bank gewesen, hätten wir beim Punkt ‚das ist eine alte Version mit bekannten Schwachstellen' aufhören müssen, die Bank hätte nie von dem ungebetenen Besuch erfahren, hätte keine Ermittlungen einleiten und die Kunden nicht warnen können. Das wäre ein großer Schaden zu Lasten der Kunden der Bank gewesen.
>
> Den angesprochenen Exploit kann man mit Hilfe von Google finden. Das kann jedes Kind.

---

[17] Die Code Blau GmbH ist ein 1999 gegründeter IT-Sicherheitsdienstleister, siehe http://www.codeblau.de/ vom 8. Juli 2008.

> Wie man in der Vergangenheit bei verhafteten Virenautoren gesehen hat, werden solche Sicherheitslücken auch häufig von Minderjährigen ausgenutzt. So einfach geht das, wenn man erst einmal das Tool dafür hat. Das ‚Hackertoolverbot' entwaffnet hier also genau die falsche Seite: den Verteidiger, nicht den Angreifer. Der Angreifer kommt typischerweise aus China, Osteuropa, der Türkei. Das ‚Hackertoolverbot' schert diese Angreifer wenig.
>
> Die neue Gesetzgebung sorgt aus unserer Sicht dafür, daß deutsche Firmen das Sicherheitsniveau nicht halten können. Wir werden nicht nur angegriffen werden, wir werden uns auch mangels Angriffstools nicht mit den Angriffsmethoden vertraut machen können. Das wird dazu führen, daß wir die Angriffe nicht bemerken. Das wird zu einem Effekt führen, wie wir ihn seit Jahren in Südkorea beobachten können: Die Mehrheit der per Breitband-Internet angebundenen Bevölkerung wurde erfolgreich angegriffen, und die Einbrecher greifen dann von den übernommenen Rechnern aus andere Ziele an. Wir gehen daher davon aus, daß das ‚Hackertoolverbot' dazu führen wird, daß Ziele im Ausland vermehrt von Computern in Deutschland aus angegriffen werden, die von Angreifern aus dem Ausland übernommen wurden.
>
> Wir sehen uns durch das ‚Hackertoolgesetz' in der Ausübung unseres Berufes eingeschränkt und befürchten starke Nachteile für den Standort Deutschland als Folge."

Von Leitners Bericht reflektiert Erfahrungen, die uns so oder ähnlich von verschiedenen Beratungsunternehmen aus der Sicherheitsbranche berichtet wurden. Die Unternehmen haben in der Mehrzahl ihr Dienstleistungsangebot reduziert, um sich nicht der Gefahr einer Kriminalisierung auszusetzen. Aufträge von ausländischen Kunden werden oft nicht mehr wie bisher von Deutschland aus bearbeitet. Kritische Aufträge von Kunden, die beispielsweise die Entwicklung von speziellen Testwerkzeugen für Sicherheitslücken beinhalten, werden an ausländische Subunternehmer vergeben, mit deutschem Personal im Ausland bearbeitet oder in Teilen abgelehnt.

Die bisher übliche Übermittlung von Testwerkzeugen mit dem Analysebericht an den Kunden, mit denen dieser nach einer Konfigurationsänderung selbständig neue Tests durchführen kann, unterbleibt aufgrund des Risikos seit der Gesetzesänderung vielfach. In der internationalen Konkurrenzsituation entsteht dadurch ein Wettbewerbsnachteil, da ausländische Anbieter diese Dienstleistung selbstverständlich anbieten.

Vielfach berichtet wird weiterhin, daß Kunden anfragen, ob nach der Gesetzesänderung der Geschäftsbetrieb noch fortgesetzt würde, wenn keine „Hackertools" mehr verwendet werden dürften. Kunden lassen sich bei Aufträgen schriftlich bestätigen, daß sie lieber weniger Sicherheitstest akzeptieren als dem möglicherweise durch Strafe bedrohten Einsatz von „Hackertools" zuzustimmen. Damit bleiben zwangsläufig Sicherheitsschwächen unentdeckt. Im Zweifel beauftragen Unternehmen nun ausländische Dienstleister, um wahrgenommene rechtliche Risiken und Unsicherheiten bei deutschen Anbietern zu vermeiden.

Neben der Anpassung von Arbeitsweise und Dienstleistungsangeboten sowie dem teilweisen Ablehnen von Aufträgen zeichnen sich noch drastischere Auswirkungen ab. Die meisten befragten Unternehmen gaben an,

einen „Plan B“ entwickelt zu haben, der eine vollständige Verlagerung der von Kriminalisierung bedrohten Dienstleistungen oder des gesamten Unternehmens ins Ausland vorsieht. Dies wird geschehen, sobald sich abzeichnet, daß es vermehrt zu Fällen von Strafverfolgung kommt, bei denen der § 202c StGB im Sinne der Buchstaben des Gesetzes interpretiert wird. Durch die bereits vielfach erfolgte Vorbereitung der Verlagerung ins Ausland ist abzusehen, daß es dann zu einer regelrechten Welle von Abwanderungen und auch zu Unternehmensverkäufen an ausländische Konkurrenten kommt, die zu weiterer Verunsicherung in der Branche führen wird.

Von allen befragten Unternehmen wurde Unverständnis darüber artikuliert, daß der Gesetzgeber, trotz ausführlicher Expertenanhörungen und Warnungen aus der Branche, eine offenbar fehlerbehaftete und realitätsfremde Gesetzesänderung beschlossen hat. Ansichten wie „offensichtlich ist IT-Sicherheit in Deutschland seitens der Regierung nicht mehr erwünscht“, wurden immer wieder geäußert. Daraus resultiert auch die hohe Bereitschaft, eine Verlagerung ins Ausland oder den Verkauf des Unternehmens an einen ausländischen Konkurrenten in Erwägung zu ziehen und konkret vorzubereiten.

4.1 Weiterbildungs- und Sensibilisierungsmaßnahmen

Wie bereits erläutert, setzen Unternehmen sowohl auf interne IT-Sicherheitsabteilungen und die Weiterbildung der Mitarbeiter als auch auf externe IT-Sicherheitsdienstleister, um die eigene IT-Infrastruktur gegen Angriffe von innen und außen zu schützen. Die Ausbildung und Sensibilisierung der eigenen Mitarbeiter und IT-Sicherheitsspezialisten ist ein kontinuierlicher Prozeß und wird in der Regel durch interne Arbeitsgruppen sowie auch durch externe Dienstleister realisiert. Eine solche Schulungsmaßnahme in einem Betrieb bewegt sich in den meisten Fällen ebenfalls in einer rechtlichen Grauzone, da hier unter anderem die Vorgehensweise von kriminellen Angreifern sowie deren Werkzeuge vorgestellt werden. Dies ist insofern wichtig bei der Sensibilisierung für solche Themen, da den meisten Schulungsteilnehmern nicht bewußt ist, welches Ausmaß an Schaden sie mit alltäglichen Werkzeugen theoretisch wie praktisch anrichten könnten.

Zur Sensibilisierung von Mitarbeitern, in deren Verantwortung das allgemeine Sicherheitsniveau eines Unternehmensnetzwerkes steht, werden typischerweise theoretische Grundlagen und Vorgehensweisen von Angreifern erläutert, aber auch die entsprechenden Werkzeuge bereitgestellt, um diese im Rahmen einer Schulung selbst zu verwenden. Nur durch die praktische Nutzung dieser Werkzeuge und Software zum gezielten Ausnutzen von Schwachstellen kann das theoretische Wissen verfestigt werden und zu einer sinnvollen Sensibilisierung beitragen.

Seit dem Inkraftreten des § 202c StGB wächst die Verunsicherung auf beiden Seiten: den Schulungsteilnehmern und den Referenten. Es war in vielen Fällen nötig, als sinnvoll erachtete, vielfach getestete Schulungsagenden anzupassen und dahingehend zu verändern, daß das Lernziel der Vertiefung des Wissens und insbesondere der Anregung weitergehender eigener Forschungen durch die Teilnehmer nun nicht mehr Bestandteil der Schulungsmaßnahmen ist. Weiterhin herrscht Unsicherheit bei den Teilnehmern, wenn ihnen die typische Sichtweise der Angreifer erläutert und zudem erörtert wird, wie sich vermeintlich harmlose Werkzeuge auch für kriminelle Zwecke mißbrauchen lassen. Die entstandene rechtliche Grauzone zwischen der Verwendung von überall verfügbarer Software wie etwa

Webbrowsern als Angriffswerkzeug einerseits oder andererseits der Verwendung von Angriffswerkzeugen wie Exploits zur Überprüfung des eigenen IT-Sicherheitsniveaus verschwimmen und entziehen sich der rationalen Erklärbarkeit.

Die logische Konsequenz eines Unternehmens auf die veränderte Rechtslage ist es, entweder vollständig auf sinnvolle Schulungsmaßnahmen im eigenen Betrieb zu verzichten oder aber die Mitarbeiter zu einer kostspieligen Schulung ins Ausland zu schicken. Schulungen zur Weiterbildung und Sensibilisierung der Mitarbeiter sind jedoch unbedingt notwendig, um sich der aktuellen Angriffsmethoden und modernen Vorgehensweisen bewußt zu werden.

Weitere Fälle, die nach Inkrafttreten des § 202c StGB rechtlich zweifelhaft geworden sind, betreffen öffentliche Vorführungen von Angriffstechniken mittels Software, deren Ziel die Kompromittierung von Servern sind. Solche „Live-Hacking“ genannten Vorträge auf kommerziellen IT-Messen mögen auf der einen Seite zwar unseriös erscheinen, da in erster Linie mittels bekannter, veralteter Techniken viel Wirbel um längst beseitigte Schwachstellen gemacht wird. Jedoch dienen sie auch hier meist der Sensibilisierung, da bislang unbedarften Personen auf anschauliche Weise praktische Probleme vorgeführt werden. Das Ziel ist es in der Regel, die Zuschauer stärker für das Thema IT-Sicherheit zu interessieren. Der Vortragende selbst ist typischerweise nicht die Person, welche die jeweiligen Schwachstellen aufgedeckt hat, jedoch kann er sich nach § 202c StGB durchaus durch solche Veranstaltungen strafbar machen.

Eine Live-Hacking-Aufführung auf einer IT-Messe oder ein Vortrag auf einer kommerziellen oder wissenschaftlichen Konferenz kann also eine Strafverfolgung nach sich ziehen, auch wenn nur die Wissensvermittlung oder Sensibilisierung intendiert war.

Im Rahmen dieser Stellungnahme wird nicht näher auf die im wissenschaftlichen Bereich entstandenen Unsicherheiten in Lehre und Forschung eingegangen.[18] Viele der beschriebenen Probleme lassen sich jedoch auf die universitäre Forschung und Bildung übertragen. IT-Sicherheitsforscher an den Universitäten können in ähnliche Konflikte zwischen ihren Dienstpflichten und der neuen Rechtslage geraten, wie sie im kommerziellen und „ehrenamtlichen“ Sektor zu beobachten sind. Eine Einschränkung von Lehre, Forschung, wissenschaftlichen Vorträgen sowie studentischer Praktika und Übungen sind die Folge.

4.2 Zertifizierung von IT-Sicherheitsforschern

Im Rahmen der Diskussion um den §202c StGB wurde in Analogie von potentiell schädlicher Software zu Gefahrstoffen vorgeschlagen, eine Art Zertifizierung bzw. Genehmigung für Forscher, Selbständige und Unternehmen zu entwickeln, denen dann der Umgang mit potentiell „gefährlicher“ Software erlaubt wäre – vergleichbar mit dem heutigen Genehmigungswesen zum Umgang mit Gefahrstoffen. Dieser Vorschlag ist auf mehreren Ebenen unpraktikabel, führt nicht zu einer Verbesserung der Situation und würde zu erheblichen negativen Folgen für die gesamt IT-Industrie führen.

---

[18] Die Problematik ist nach dem Kenntnisstand der Autoren Grundlage einer weiteren Verfassungsbeschwerde.

Zum einen läßt sich, wie bereits dargelegt, eine eindeutige Zweckbestimmung für Software prinzipiell nicht begründen. Die Aufstellung einer Kategorie „Schadsoftware“ ist nicht wissenschaftlich abgesichert, ohne die Betrachtung der Umstände und des Umfelds der Verwendung läßt sich keine eindeutige Aussage über ihren Zweck und ihre Schädlichkeit treffen.

Im Gegensatz dazu gibt es im Bereich der Chemie wissenschaftlich fundierte, allgemein anerkannte Grundsätze der Gefahrstoffklassifikation, die sich in den entsprechenden Listen und Genehmigungskategorien niederschlagen. Für die Herstellung solcher Substanzen ist eine Reihe von gut identifizierbaren Ausgangsstoffen und gegebenenfalls Instrumenten und Werkzeugen notwendig, die entsprechend reguliert werden können. Für die Herstellung von potentiell schädlicher Software ist jedoch lediglich ein Computer, Zeit sowie Wissen erforderlich. Im übrigen verkennt die Gefahrstoff-Analogie, daß die Regeln für den Umgang mit Gefahrstoffen für die Vermeidung von Unfällen und Katastrophen erstellt wurden, jedoch kaum einen wirksamen Schutz gegen absichtliche Beschaffung, Herstellung und Verwendung der Stoffe bietet.

Die Einführung eines Zertifikats oder einer Genehmigung für den Umgang mit potentiell schädlicher Software steht weiterhin vor dem grundlegenden Problem, daß neben der nicht möglichen Klassifizierung von Software in eindeutige Schädlichkeitskategorien die Innovationsfähigkeit und sogar der Bestand der deutschen IT-Sicherheitsindustrie stark gefährdet würde. Ebenso wie durch die nun entstandene überzogene Rechtslage bezüglich der „Hackertools“ schadet ein solcher Ansatz dem IT-Standort Deutschland.

Die deutsche IT-Sicherheitsbranche besteht neben den bekannten großen und mittleren Unternehmen vor allem aus inhabergeführten Klein- und Kleinstbetrieben, in denen ein wesentlicher Anteil der innovativsten Sicherheitsforschung geleistet wird. Die Firmen sind gelegentlich im universitären Umfeld angesiedelt, verfügen oft auch über gute Kontakte in die Grauzonen der „Szene“ und rekrutieren hier ihre talentiertesten Mitarbeiter. Etwaige behördliche Kriterien für die Erteilung einer Genehmigung, anhand derer die „Zuverlässigkeit“ des Antragstellers beurteilt würde, führte daher mit hoher Wahrscheinlichkeit zum Ausschluß eines Großteils der begabtesten Sicherheitsforscher.

Hier findet jedoch der intensivste Informationsaustausch über neue Angriffsvektoren statt, neue Produkte und Methoden zur Abwehr werden entwickelt und dann häufig an größere Unternehmen lizenziert oder verkauft, die diese Komponenten dann unter ihrem eigenen Namen vertreiben. Die neue Gesetzgebung mit der entstandenen rechtlichen Grauzone hat die Abwanderung kompetenter Sicherheitsforscher durch das Risiko der Kriminalisierung bereits verstärkt.

Für diese Personen und Kleinunternehmen ist aber auch ein behördliches Zertifizierungsverfahren für potentiell schädliche Software nicht gangbar. Vor die Wahl gestellt, sich mit einem aufwendigen und teuren bürokratischen Prozeß mit fachlich unsinnigem Ziel zu befassen, würden weitere der betroffenen Personen und Firmen ins Ausland abwandern. Die Bereitschaft, sich durch offensichtlich nicht zielführende Maßnahmen – sei es eine überzogene Strafgesetzgebung oder eine zwangsweise Zertifizierung – gängeln zu lassen, ist in dieser Branche äußerst gering ausgeprägt. Vor dem Hintergrund der starken internationalen Nachfrage nach kompetenten IT-Sicherheitsexperten und dem entsprechendem finanziellen Anreiz

besteht Grund zur Annahme, daß Deutschland einen wesentlichen Teil der Innovationsbasis seiner IT-Sicherheitsindustrie verliert.

Weite Teile der bisher durchaus offen agierenden und frei publizierenden, aber nicht etablierten Sicherheitsforschung sind Personen, die sich aus eigenem Interesse und ohne kommerziellen oder universitären Hintergrund mit Fragen der Computersicherheit befassen. Diese bisher offen Sicherheitslücken dokumentierende „Szene“, in die der Chaos Computer Club gute Kontakte pflegt, hat bereits Konsequenzen aus der Gesetzgebung gezogen und droht infolge der Kriminalisierung oder zwangsweisen Zertifizierung, vollständig in den virtuellen „Untergrund“ zu verschwinden.

Die etablierten IT-Sicherheitsunternehmen verlieren damit den Anschluß an den Informationsfluß hinsichtlich neuer Probleme im Bereich IT-Sicherheit. Verzichten sie aber auf Praxistests und Forschung nach dem aktuellen Stand der Angriffsvektoren, nehmen sie Datenverluste oder anderweitige Schäden an der IT-Infrastrultur in Kauf, sie haften dafür sogar gegebenenfalls entsprechend.

Wenn in Deutschland Informationen über eine neue Sicherheitslücke publiziert oder an einen Hersteller übergeben werden, sieht sich der Veröffentlicher potentiell sofort strafrechtlicher Verfolgung ausgesetzt. Demzufolge unterbleibt die Publikation. Dieser Effekt der neuen, praxisfernen Gesetzeslage würde sich durch ein Zertifizierungsverfahren noch verstärken.

Die Publikation von Sicherheitslücken ist also von einer großen Rechtsunsicherheit bedroht. Im Zweifel werden gefundene Sicherheitslücken daher nicht dem Hersteller oder einem spezialisierten Dienstleister mitgeteilt, sondern nur „unter der Hand“ an Gleichgesinnte weitergegeben oder getauscht. In der Folge bleiben die Lücken dem Hersteller unbekannt, können nicht geschlossen, jedoch von kriminellen Angreifern ausgenutzt werden, ohne daß diese eine Entdeckung befürchten müssen.

4.3 Verfügbarkeit von Informationen über Sicherheitslücken

Durch die unscharfe Formulierung des § 202c StGB sind, wie von den Experten in den Anhörungen des Rechtsausschusses des Bundestages vor Verabschiedung des Gesetzes vorhergesagt, eine Reihe von Effekten eingetreten, welche die Computersicherheit für die Allgemeinheit verschlechtern. Eine gravierende Auswirkung ist die Einschränkung des Angebots an Informationen und Werkzeugen für die Verbesserung der Sicherheit des eigenen Systems. Seit Inkrafttreten des Gesetzes ist eine massive Verunsicherung darüber spürbar geworden, welche Publikationen noch rechtlich unkritisch sind. Dies manifestiert sich gerade in den Publikationen und Online-Medien, die dem Thema IT-Sicherheit bisher große Aufmerksamkeit widmeten.

Der Heise Zeitschriften Verlag mit dem Informationsportal „heise online“ und der Zeitschrift „c‘t – Magazin für Computertechnik“ ist in Deutschland die wichtigste aktuelle Informationsquelle für IT-Sicherheitsthemen. Um die entstandene Problematik durch die neue Gesetzgebung zu verdeutlichen, sei hier beispielhaft ein Brief des Chefredakteurs von heise Security und Leitenden Redakteurs von „c‘t – Magazin für Computertechnik“, Jürgen Schmidt, zitiert. Schmidt beschreibt die Auswirkungen des § 202c StGB auf den Redaktionsalltag:

„Die neuen Gesetze im Bereich Computerkriminalität und dabei insbesondere der sogenannte ‚Hackerparagraph' 202c StGB haben zu einer erheblichen Behinderung unserer redaktionellen Arbeit geführt, die ich als Einschränkung der Pressefreiheit betrachte.

Bei stichprobenartigen Befragungen meiner Kollegen stellte ich fest, daß außerhalb des Security-Bereichs die Auswirkungen auf die redaktionelle Arbeit hauptsächlich im Vorfeld der Veröffentlichung zu beobachten sind. So kommt es eher selten zu Situationen, in denen man beispielsweise einen Link wegen diesbezüglicher Überlegungen in letzter Minute dann doch wieder entfernt.

Viel öfter werden potentiell kritische Links oder Tools, die im direkten Zusammenhang mit einer Veröffentlichung stehen, erst gar nicht berücksichtigt, etwa weil man nicht die Zeit für langwierige Nachfragen bei der Rechtsabteilung hat. Exemplarisch sei hier die Zusammenstellung von Software für unser Software-Verzeichnis (http://www.heise.de/software/) genannt, wo ein Assistent eine harmlose Inventarisierungssoftware, die auch die MAC-Adressen der PCs erfaßt, ‚vorsichtshalber' nicht aufgenommen hatte. Seine Begründung war, das könne doch auch zum Hacken mißbraucht werden.

Vor allem im Security- und Netzwerk-Bereich läßt sich eine noch konkretere Behinderung unserer Arbeit beobachten. Beispielhaft möchte ich vier konkrete Fälle dokumentieren, in denen Erwägungen rund um den Paragraphen 202 StGB unseren Redaktionsalltag beeinflußt und die Berichterstattung behindert haben.

1) Wir führen regelmäßige Tests von Anti-Viren-Software durch. Um die Qualität dieser Programme zu testen, erstellten wir bislang immer Variationen bekannter Schädlinge und implementierten auch einfache Schadfunktionen, wie etwa einen Keylogger, selbst beziehungsweise ließen das im Auftrag entwickeln. Das erlaubt uns Aussagen, wie leicht sich Anti-Viren-Software austricksen läßt beziehungsweise wie gut sie auch bislang unbekannte Schädlinge erkennt. Diese ‚Test-Viren' existieren nur in unserem Tresor. Trotzdem machte ich mich nach Auskunft unserer Rechtsabteilung durch dieses Vorgehen unter Umständen strafbar. Ohne diese Tests fehlt jedoch ein wesentliches Qualitätsmerkmal unserer Testberichte. Die letzten Kurztests wurden ohne ‚Test-Viren' durchgeführt; wie wir im nächsten großen Vergleichstest vorgehen, ist bislang noch offen. Das Resultat: Sinnvolle Tests von Anti-Viren-Software unterbleiben.

2) SSH-Keys: In der Diskussion rund um die verwundbaren OpenSSL-Keys wurde sehr schnell klar, daß derzeit allein in Deutschland tausende von Servern konkret verwundbar sind.[19]

Nicht klar war, wie real die Gefahr ist. Das Knacken eines Accounts könnte wenige Minuten, aber auch durchaus Wochen oder Monate dauern. Um dies abzuschätzen, hätte man ein Tool schreiben müssen, das genau dies real probiert – selbstverständlich an einem von uns installierten Testsystem. Nach kurzer Rücksprache mit unserer

[19] Gemeint ist die in Kapitel 1.4 angesprochene Debian-Problematik, siehe http://www.heise.de/security/news/meldung/108528/ vom 9. Juli 2008.

> Rechtsabteilung haben wir von diesem Test abgesehen. Es ist bis heute offen, wie lange ein solcher Angriff dauert. Und es sind immer noch hunderte, wenn nicht tausende Server verwundbar. Das Resultat: Eine unter Umständen erforderliche Warnung der Öffentlichkeit erfolgt nicht.
>
> 3) Wir drehten einen Webcast, der demonstrieren sollte, wie schnell die einfache WEP-Verschlüsselung von Funknetzen geknackt werden kann und zur Verwendung besserer Verfahren animieren sollte. Die Dreharbeiten waren ein einziger Eiertanz, weil nie ganz klar war, was man zeigen kann, ohne sich strafbar zu machen. Das Ergebnis entsprach dann unter anderem deshalb unseren Anforderungen nicht, sodaß eine Veröffentlichung unterblieb. Das Resultat: Ein Aufklärungsvideo, das vor Gefahren warnen sollte, wurde nicht veröffentlicht.
>
> 4) Die Begleit-DVD für das c't-Netzwerk-Sonderheft 1/08 wurde mit explizitem Verweis auf den ‚Hackerparagraphen' und das damit verbundene Risiko für uns um folgende Tools bereinigt:
>
> airsnort, crack, fcrackzip, hydra, john, rainbowcrack, sucrack, ophcrack, aircrack-ng, crack-common, cracklib-runtime, grml-sectools, ike-scan, libwhisker-perl, nikto, wapiti.
>
> Das heißt, diese Tools waren für eine Veröffentlichung vorausgewählt, zum Teil, weil sie auch schon auf früheren CDs enthalten waren, wurden dann aber wegen der unklaren Rechtslage vorsichtshalber entfernt. Das Resultat: Netzwerk-Adminstratoren werden nicht über öffentlich verfügbare Tools informiert, die ihnen helfen können, Gefahren zu verstehen und ihre Systeme und Netze besser zu sichern.
>
> Zusammenfassend stelle ich fest, daß sich die aktuelle Gesetzgebung im Bereich Computerkriminalität und dabei insbesondere der Paragraph 202c StGB massiv auf unsere redaktionelle Arbeit auswirkt. Durch die bestehende Rechtsunsicherheit können wir einen Teil unserer Aufgaben als unabhängiges Medium im Sinne einer freien Presse nur noch eingeschränkt wahrnehmen."

Die von Jürgen Schmidt genannten Beispiele und Vorgänge sind exemplarisch für die Presse, aber auch für den gesamten Bereich der Industrie. Die Rechtsabteilungen der Unternehmen wollen verständlicherweise Risiken minimieren und neigen daher zu einer pessimistischen Interpretation der Rechtslage. Im Zweifel wird eher von der Publikation von Informationen und Werkzeugen abgesehen, die möglicherweise als „Angriffswerkzeug" interpretiert werden können. Schneller und ungehinderter Informationsfluß ist jedoch vollständig unabdingbar für die Abwehr von Computerangriffen.

Ein weiteres konkretes Beispiel für die entstandene Rechtsunsicherheit zeigt sich bei Werkzeugen, welche Paßwörter per brute-force-Methode[20] entschlüsseln. Die Frage, ob sich der Entwickler strafbar macht, wenn er

[20] Eine brute-force-Methode testet alle möglichen Varianten (vollständige Enumeration).

eine solche Software schreibt oder zur Verfügung stellt, ist derzeit noch immer ungeklärt.[21]

Mangelndes oder veraltetes Wissen und nur auf kompliziertem Wege verfügbare Werkzeuge sind die häufigsten Ursachen für nicht gestopfte Sicherheitslücken, die dann von kriminellen Angreifern ausgenutzt werden können. Angesichts der Fülle von mehr oder weniger wichtigen Nachrichten im Bereich der IT-Sicherheit spielt die ausführliche und vollständige Behandlung von kritischen Problemen in Leitmedien wie denen des Heise Zeitschriften Verlages eine wesentliche Rolle. Viele Systemadministratoren verlassen sich darauf, daß sie die notwendigen Informationen und Werkzeuge zum Test, ob ihr System von einer neuen Lücke betroffen ist, auf diesem Wege erhalten. Durch die Beschränkung der Publikation ist der Systemverantwortliche dazu gezwungen, sich die notwendigen Informationen auf ausländischen Seiten zu besorgen oder nicht vertrauenswürdige Quellen für die Beschaffung von Testwerkzeugen zu wählen. Dieser Aufwand wird von vielen Administratoren nicht betrieben, da dadurch ihre ohnehin hohe Arbeitsbelastung weiter ansteigt. In der Folge sind Systeme schlechter gesichert, Lücken werden nicht erkannt oder als nicht für relevant erachtet.

Für kriminelle Angreifer stellt die Beschaffung von Werkzeugen und Informationen hingegen kein wirkliches Problem dar, für sie steigt der Aufwand nur marginal, da sie diese in der Regel aus nicht-öffentlichen oder ausländischen Quellen beziehen oder ausreichend eigene Expertise für die Erstellung von Angriffswerkzeugen haben. Durch die in der Summe gesunkene Systemsicherheit und den geringeren Informationsstand der verantwortlichen Mitarbeiter ergeben sich mehr und schwerwiegendere Angriffsmöglichkeiten.

Im Ergebnis erschwert die gegenwärtige Situation also die Arbeit der Verteidigung und senkt die Sicherheit der Systeme gegen Computerangriffe – das genaue Gegenteil der vom Gesetzgeber intendierten Effekte.

Insbesondere die Möglichkeiten, Computersicherheitssoftware von deutschen Webseiten zu laden, haben sich reduziert. Die Download-Bereiche bekannter Webseiten, die regelmäßig und zeitnah über Fragen der IT-Sicherheit informieren, sind drastisch reduziert, teilweise geschlossen worden.[22] Softwareentwickler haben vergleichbare Schritte ebenfalls vor-

---

[21] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf der CD „BSI OSS Security Suite“ ein solches Programm mit dem Namen „John the Ripper“ an. Der IT-Online-Nachrichtendienst tecChannel.de erstattete nach der Strafrechtsänderung Anzeige gegen das BSI. Im Oktober 2007 hatte die Staatsanwaltschaft Bonn verneint, daß das BSI mit „John the Ripper“ einen Straftatbestand erfüllt. Da die gelieferte Begründung nicht dazu geeignet war, Rechtssicherheit hinsichtlich § 202c StGB zu schaffen, legte tecChannel.de Beschwerde beim Oberstaatsanwalt ein. Siehe http://www.tecchannel.de/sicherheit/news/1737683/index.html vom 13. Juli 2008.

[22] So hat etwa die Hackergruppe „Phenoelit“, die international durch die Aufdeckung und die Veröffentlichung erheblicher Sicherheitslücken bekannt wurde, bereits Konsequenzen aus der veränderten Gesetzgebung gezogen und ihre deutsche Webseite geschlossen. Siehe http://www.phenoelit.de/202/202.html vom 9. Juli 2008. „Much to our regret, this site is no longer available in the form it has been since the late 1990s. It became illegal.“

genommen und bieten ihre Software nicht mehr an (so etwa der Entwickler des Programms KISmac[23]).

Das Computer Emergency Response Team Coordination Center (CERT/CC) der US-amerikanischen Carnegie Mellon Universität veröffentlichte im Jahr 2006 insgesamt 8.064, im Jahr 2007 jedoch nur noch 7.236 neu bekanntgewordene Schwachstellen.[24] Daß seit Erstellung der Statistik im Jahr 1995 die Anzahl der jährlich gemeldeten Schwachstellen etwa um den Faktor 2 angewachsen ist, in jüngster Zeit jedoch ein Rückgang der gemeldeten Sicherheitslücken zu verzeichnen ist, kann auf die restriktivere Gesetzgebung in einigen Ländern und die reduzierte Veröffentlichungsbereitschaft zurückgeführt werden. Weniger tatsächliche Angriffe oder finanzielle Schäden durch Schwachstellen sind jedoch nicht zu verzeichnen.[25] Die Anzahl eingesetzter Software und zwangsläufig entsprechend enthaltener, aber nicht gemeldeter Schwachstellen ist bei realistischer Betrachtung keineswegs rückläufig. Jedoch ging die Anzahl der Veröffentlichungen über gefundene Schwachstellen in den letzten Jahren zurück.[26]

Rechtliche Grauzonen wie die des § 202c StGB können immer zweiseitig gedeutet werden. Dies führt auch in Deutschland zu einem Rückgang der Veröffentlichung gefundener Schwachstellen. Auf der einen Seite kann der Paragraph so ausgelegt werden, daß ehrliche Menschen, deren Beruf es ist, mit „Hackertools“ zu hantieren, selbstverständlich nicht rechtlich dafür belangt werden. Auf der anderen Seite müßte sich dieselbe Person jedoch im Zweifelsfall zunächst dafür rechtfertigen, solche Werkzeuge überhaupt zu besitzen, weitergegeben oder selbst entwickelt zu haben.

In einer gerichtlichen Auseinandersetzung kann es also leicht dazu kommen, daß ganz unabhängig vom Beruf der Person unter anderem der Besitz von „Hackertools“ als negatives Indiz gewertet wird. Ebenso wie bei Privatpersonen verhält es sich bei Unternehmen. Durch die überzogene Formulierung im § 202c StGB besteht je nach Auslegung das Risiko eines erheblichen finanziellen Schadens für das Unternehmen, wenn Mitarbeiter „Hackertools“ einsetzen oder entwickeln.

Der Gesetzgeber ist mit dem Wortlaut weit über die Grenzen der Verfassung hinausgeschossen. Betrachtet man den reinen Wortlaut, so ist es nicht nur theoretisch möglich, jede Benutzung, Entwicklung und Weitergabe potentiell schädlicher Software zu untersagen und mithin Benutzer und Programmierer zu kriminalisieren. Der Wortlaut führt zu einem mißverständliches Gesetz, das kaum eine einschränkende Auslegung zuläßt.

---

[23] Das Programm sucht nach drahtlosen Funknetzen, siehe http://kismac.de/ vom 9. Juli 2008. „With the introduction of § 202c German politicians proved their complete incompetence.“

[24] CERT/CC: Vulnerability Remediation Statistics, siehe http://www.cert.org/stats/vulnerability_remediation.html vom 11. Juli 2008.

[25] Vgl. Computer Security Institute: Computer Crime and Security Survey, 2007.

[26] CERT/CC: Vulnerability Remediation Statistics, siehe http://www.cert.org/stats/vulnerability_remediation.html vom 11. Juli 2008.

5 Fazit

Eine Unterscheidung, welchen Zweck eine Software verfolgt, ist aus informationstechnischer Sicht nicht möglich. Es gibt keine objektiven Kriterien, anhand derer sich festmachen ließe, daß ein Programm ausschließlich legalen oder illegalen Absichten dient. Wie bei einem mechanischen Werkzeug, etwa einem Skalpell oder einem Hammer, entscheidet erst die Verwendung durch den Anwender über den Zweck und die mögliche Strafbarkeit des damit ausgeführten Handelns.

Angesichts der Verschiedenartigkeit und Komplexität von Computern und Netzwerken ist eine unüberschaubare Vielfalt von Programmen und Softwarekomponenten entstanden, die für den Betrieb von IT-Systemen notwendig sind, sich aber auch für illegale Zwecke einsetzen lassen. Die Mehrzahl der Angriffe im Internet erfolgt mit Hilfe solcher „dual-use"-Werkzeuge – bis hin zum normalen Webbrowser.

Beruhend auf dem Recht zum digitalen Selbstschutz, das sich aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergibt, müssen die Bürger und die Wirtschaft in der Lage bleiben, ihre Computersysteme auf Sicherheitslücken zu testen. Dazu ist der Besitz von Angriffswerkzeugen unabdingbar notwendig.

Für IT-Berater und IT-Sicherheitsfirmen besteht der Bedarf, die sogenannten Angriffswerkzeuge zu besitzen sowie mit ihnen zu experimentieren und sie weiterzuentwickeln. Weiterhin ist es unabdingbar, sich (auch öffentlich) mit anderen IT-Spezialisten über Sicherheitslücken und Wege zu ihrer Ausnutzung auszutauschen. Dazu muß den Computersicherheitsexperten die Möglichkeit eröffnet bleiben, eigene Erweiterungen von Angriffssoftware sowie Anregungen für zukünftige Angriffe öffentlich publizieren und diskutieren zu können.

Nur hierdurch ist es möglich, aus eigenen Fehlern zu lernen, sich selbst weiterzubilden und Wissen sinnvoll in IT-Sicherheitsabteilungen und Unternehmen anzuwenden. Dies gilt gleichermaßen für externe Berater und für interne Mitarbeiter eines Unternehmens, ebenso für sich selbst weiterbildende Studierende und Berufseinsteiger.

Neu gefundene Sicherheitslücken müssen in der Regel durch Testsoftware, die diese Schwachstellen ausnutzen, belegt werden, da sonst nicht die notwendige Aufmerksamkeit und Reaktion von Herstellern und Anwendern zu erreichen ist.

Der Besitz und Austausch von Software, für die sich ein überwiegend schädlicher Charakter begründen läßt, wie etwa Viren und Trojaner, ist für den Erhalt der Systemsicherheit ebenfalls zwingend notwendig, da nur durch die Analyse dieser Software ihre Verbreitung durch Gegenmaßnahmen einzudämmen ist. Diese Gegenmaßnahmen werden zunehmend von den betroffenen Unternehmen, wie etwa Banken, selbst entwickelt. Eine Kriminalisierung des Umgangs mit Schadsoftware führt daher zu einer direkten Senkung des allgemeinen Niveaus der IT-Sicherheit in Deutschland. Die Ausbildung neuer Sicherheitsfachleute wird massiv erschwert und eine Abwanderung der talentiertesten Forscher und Entwickler ins Ausland ist heute bereits absehbar, wenn die derzeit geltende Gesetzeslage bestehen bleibt.

Eine Beschränkung des Zugangs zu Schadsoftware ist nicht mit juristischen Mitteln realisierbar. Allein durch normale E-Mailbenutzung werden jeden Tag verschiedenartigste Schadprogramme empfangen, die problemlos modifiziert und für kriminelle Zwecke verwendet werden können. Werkzeuge sind zudem frei aus dem Internet herunterladbar.

Kriminelle, die bekannte oder noch unbekannte Sicherheitslücken ausnutzen, müssen ohnehin mit Strafverfolgung rechnen und agieren dementsprechend konspirativ. Eine technische Einschränkung des Zugangs würde eine vollständige Internet-Überwachung erfordern, die zweifelsfrei verfassungswidrig wäre. Da zudem statistisch gesehen die meisten Angriffe mit eher trivialen oder „dual-use"-Werkzeugen ausgeführt werden, wäre selbst so ein vollkommen unangemessenes Mittel nicht geeignet, die Anzahl der Angriffe zu reduzieren.

Die bisherigen Auswirkungen des § 202c StGB in der Praxis reichen von der Selbstbeschränkung wichtiger Medien im Bereich der IT-Sicherheit über die Abwanderung von Sicherheitsforschern bis zur effektiven Einschränkung der akademischen Forschung und Lehre. Die Einschränkung des Informationsangebots über Sicherheitslücken in deutschsprachigen Publikationen reduziert langfristig das allgemeine Sicherheitsniveau. Die entstandene Rechtsunsicherheit hat sich bereits für die ansonsten international gut aufgestellte deutsche IT-Sicherheitsbranche zu einem Geschäftshindernis entwickelt, da häufig Nachfragen von verunsicherten Kunden beantwortet werden müssen. Sicherheitsberatungsunternehmen haben bereits ihre Dienstleistungen eingeschränkt und übergeben beispielsweise die Testprogramme für gefundene Sicherheitslücken nicht mehr an den Auftraggeber. Dadurch wird das Leistungsspektrum und damit die Konkurrenzfähigkeit der deutschen Unternehmen eingeschränkt. Die Auftraggeber sind nicht mehr in der Lage, gefundene Lücken nachzuvollziehen und beispielsweise nach einer Umkonfiguration selbst neu zu prüfen.

Behörden und Unternehmer, die von Privatpersonen auf Lücken aufmerksam gemacht werden, reagieren nicht immer mit Dankbarkeit auf das Aufdecken dieser Probleme. Dadurch, daß die Betroffenen einem gewissen Rechtfertigungszwang aufgrund eigener Fehler unterliegen, versuchen sie verstärkt, den Überbringer der unangenehmen Botschaft für das gefundene Sicherheitsloch verantwortlich zu machen. Dadurch entstand schon nach der alten Rechtslage ein nicht unerhebliches Risiko eines Ermittlungsverfahrens gegen den „Finder".

Dieser Effekt hat sich mit dem § 202c StGB noch verstärkt. Im Ergebnis geht die freiwillige Preisgabe entdeckter Sicherheitsprobleme weiter zurück. Professionelle wie auch „ehrenamtliche" Hacker überdenken aufgrund der hohen Strafandrohung, ob sie sich einem solchen Risiko aussetzen wollen. Damit wird in Zukunft eine tatsächliche Sicherheitsüberprüfung nur durch Kriminelle möglich sein – daß diese die gefundenen Sicherheitslücken veröffentlichen und so die Behebung der Probleme ermöglichen, steht jedoch nicht zu erwarten.

Die bisherige Haltung der meisten Großunternehmen ist eher abwartend. Viele gehen davon aus, daß der § 202c StGB ohnehin keinen Bestand haben wird. Sie haben jedoch bereits alternative Strategien ausgearbeitet, welche die Verlagerung von kritischen Teilen der Forschungs- und Dienstleistungsbereiche ins Ausland vorsehen. Diese Abwanderung wird voraussichtlich zügig geschehen, sobald erste Urteile ergehen, die sich an dem

Wortlaut des § 202c StGB orientieren und die befremdlichen „das haben wir aber so nicht gemeint“-Kommentare des Gesetzgebers ignorieren.

Die Intention des Gesetzgebers und auch der dem Gesetz zugrundeliegenden Cybercrime Convention war es, eine Verbesserung der IT-Sicherheitslage durch die Beschränkung des Zugangs zu Schadsoftware und Angriffswerkzeugen zu erreichen. Die derzeitige Fassung des § 202c StGB erreicht in der Gesamtschau das Gegenteil. Die abstrakte Kriminalisierung von Softwareherstellern und -benutzern, für deren Werkzeuge sich ein Zweck grundsätzlich nicht definieren läßt, führt zu einer Senkung des Sicherheitsniveaus. Gleichzeitig folgt daraus ein Standortnachteil für die deutsche Forschung und Wirtschaft.

Die Strafnorm des § 202c StGB ist daher in der Praxis weder zielführend noch geeignet, das gesetzte Ziel zu erreichen.