SABRE Labs GmbH
Wrangelstrasse 4
10997 Berlin
http://www.sabre-labs.com

Stellungnahme

zum

Gesetzentwurf der Bundesregierung zu einem Strafrechts-änderungsgesetz zur Bekämpfung der Computerkriminalität (BT-Drs. 16/3656)

Felix Lindner
Geschäftsführer
SABRE Labs GmbH
Unternehmensberatung, Spezialgebiet EDV-Sicherheit

Berlin, 19.03.2007

SABRE Labs GmbH
Wrangelstrasse 4
10997 Berlin
http://www.sabre-labs.com

1 Einleitung

Diese Stellungnahme betrachtet die fachlichen Aspekte des Gesetzentwurfs in Hinsicht auf die wahrscheinlichen Auswirkungen bei Verabschiedung in der momentan vorliegenden Fassung. Es wird ausschließlich auf den geplanten § 202c StGB eingegangen.

2 Zu § 202c StGB

Die Bundesregierung hat in ihrem Gesetzentwurf die Definition der unter Strafe zu stellenden Computerprogramme in Abs. 2 abweichend von der Formulierung der EU Cybercrime Convention Art. 6 gewählt. Dort heißt es:

„*a device, including a computer program, designed or adapted **primarily** for the purpose of committing any of the offences […]*“,

während es in der Gesetzesvorlage heißt:

„*Computerprogramme, deren Zweck die Begehung einer solchen Tat ist […]*“

ohne dass die weitaus klarere Abgrenzung der EU übernommen wurde. Auch die Gesetzesbegründung stellt nicht das Primärmerkmal des Angriffstools heraus, vielmehr heißt es dort:

„*Das Programm muss aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reicht, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist.*“

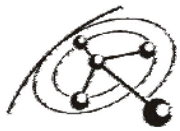
Da sowohl der Besitz als auch die Herstellung oder Verbreitung solcher Programme unter Strafe gestellt werden soll, ist die Abgrenzung der objektiven Zweckbestimmung von außerordentlicher Wichtigkeit. Im Folgenden soll kurz aufgeführt werden, welche Programme mit der Formulierung gemeint sein könnten, die heutzutage sowohl bei kriminellen als auch bei nicht kriminellen, also behördlichen und privatwirtschaftlichen, Anwendern zum Einsatz kommen.

2.1 Sicherheitstechnisch relevante Computerprogramme

Für die nachfolgende Liste ist wichtig zu bemerken, dass für alle hier genannten Softwarearten, mit Ausnahme von Viren und Würmern, kommerzielle Produkte von renommierten Unternehmen aus Deutschland, der EU oder Nordamerika angeboten werden. Es handelt sich also durchaus nicht ausschließlich um „leicht aus dem Internet zu beschaffende“ Werkzeuge von Kriminellen.

2.1.1 Scanner

Unter dem Oberbegriff der „Scanner“ werden in der IT – Sicherheit alle Programme zusammengefasst, welche einige oder alle möglichen Kombinationen von Computeradresse und Dienstmerkmal auf das Vorhandensein eines Dienstes prüfen. Dieser Vorgang kann auf verschiedenen Abstraktionsebenen von Kommunikationsnetzen durchgeführt werden, wird aber meist zur Identifikation von Diensten verwendet, welche über ein Netzwerk bereitgestellt werden.



2.1.2 Vulnerability Scanner

Ein Vulnerability Scanner ist eine Software, welche ein Zielsystem oder –netz auf bekannten Schwachstellen untersucht. Diese Schwachstellenuntersuchung kann durch die Abfrage von Informationen aus dem Zielsystem oder durch den Versuch des Auslösens einer Schwachstelle durchgeführt werden. In einigen Fällen ist selbst der Hersteller des Vulnerability Scanners nicht in der Lage, eine solche Abgrenzung anzugeben.

2.1.3 Fuzzer

Ein so genannter Fuzzer ist ein Programm, welches Eingaben für ein anderes Programm auf demselben oder einem anderen Computer generiert. Die generierten Eingaben sind Testfälle für die Stabilität und Verlässlichkeit des überprüften Programms und bestehen meist aus Grenzfällen der erwarteten Eingabe, zum Beispiel überlange Zeichenketten.

2.1.4 Sniffer

Bei Sniffern handelt es sich um Mitschnittsoftware für Netzwerkkommunikation. Sie ermöglicht das Aufzeichnen und selektive Anzeigen beziehungsweise automatische Auswerten von Daten, welche über eine Kommunikationsverbindung übertragen wurde.

2.1.5 Cracker

Ein Cracker Programm führt eine erschöpfende oder nicht erschöpfende Suche nach gültigen Schlüsseln oder Passworten auf einer lokalen oder entfernten Datenbasis durch und identifiziert hierdurch schwache Schlüssel oder Passworte.

2.1.6 Exploit

Bei einem Exploit handelt es sich um die automatisierte Ausnutzung einer Sicherheitslücke durch gezieltes anwenden des Fehlerfalls zur Erlangung von erhöhten Privilegien auf dem betroffenen System. Die Ausprägungen von Exploits sind vielfältig, die gängigen Vertreter führen hierbei vom Anwender des Exploits eingeschleusten Programmcode auf dem betroffenen System aus.

2.1.7 Exploit Framework

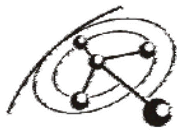
Bei einem Exploit Framework handelt es sich um eine Sammlung von Exploits (vgl. 2.1.6), welche in Kombination auf ein Zielsystem angewendet werden.

2.1.8 Agent

Bei einem Agent handelt es sich um einen Programmcode, welcher zum weiteren Verbleib auf einem Computersystem geschaffen wurde. Dieser kann über die verschiedensten Wege in das System eingeschleust werden und eine Reihe von Aufgaben bedienen. Eine gängige Aufgabe ist das Anbieten eines alternativen Zugriffsmechanismus, eine weitere das ausspionieren von Daten.

2.1.9 Virus & Wurm

Bei einem Virus handelt es sich um selbst replizierenden Code, welcher sich auf einem Computersystem verbreitet. Von einem Wurm spricht man, wenn die Replik auch über eine Netzwerkverbindung auf einem entfernten Computersystem herge-



stellt werden kann. Gängige Würmer verwenden Exploits (vgl. 2.1.6), um Zugriff auf die entfernten Systeme zu erlangen.

2.2 Abgrenzung

Basierend auf der Gesetzesvorlage ist es nicht möglich, die unter 2.1 genannten Softwarearten in strafrechtlich relevante oder als harmlos anzusehende zu unterscheiden.

Systemadministratoren und Sicherheitsberater verwenden zum Beispiel Exploit Frameworks (z.B. die Produkte „Core Impact“ oder „Immunity Canvas“), welche auch Agenten enthalten, um die Auswirkungen eines erfolgreichen Angriffs auf ein Unternehmensnetzwerk zu testen. Dieselbe Software könnte – ohne jegliche Modifikation – auch von kriminellen Anwendern verwendet werden, um in ein Netzwerk einzudringen. Die Herstellung einer solchen Software könnte also durchaus mit der in Aussichtnahme einer Straftat verbunden sein, oder auch nicht.

Bei der Analyse von Netzwerkfehlern oder Anomalien sind Sniffer unabdingbare Werkzeuge. Sie werden von Privatanwendern und Unternehmen eingesetzt, um die tatsächliche Kommunikation auf dem zu untersuchenden Kanal zu überwachen. Alle bekannten Sniffer unterstützen zur Auswertung die Funktionalität, nur bestimmte Kommunikationsbeziehungen zu analysieren. Diese Funktionalität kann ohne weiteres verwendet werden, um automatisch Passworte aus dem Netzwerkverkehr zu extrahieren und auf einen Datenträger zu speichern. Es ist praktisch unmöglich, die Intention hinter einer solchen Handlung als Vorbereitung einer Straftat nachzuweisen oder zu wiederlegen.

Weiterhin ist für den vorliegenden Gesetzesentwurf unklar, ob die korrekte Funktionalität der Software vorausgesetzt wird. Wird zum Beispiel ein Exploit oder Wurmprogramm manuell in Umlauf gebracht, dessen Kernfunktionalität – also der erfolgreiche Angriff auf ein entferntes Computersystem – mit Absicht beschädigt wurde, so ist nicht klar, ob es sich hierbei um ein nach § 202c StGB strafbares Computerprogramm handelt oder nicht. Die Veränderung eines Programms um ein einziges Bit ist gleichbedeutend mit der Neuerschaffung eines Computerprogramms, da nicht eindeutig und zweifelsfrei nachgewiesen werden kann, dass ein Programm auf einem anderen aufbaut oder eine Modifikation dessen ist.

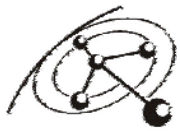
2.3 Auswirkungen von § 202c E-StGB

2.3.1 Fehlende Rechtssicherheit für Unternehmen

In Art. 6, Abs. 2 der EU Cybercrime Convention heißt es:

„*This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.*“

In der vorliegenden Gesetzesfassung wird eine solche Unterscheidung nicht getroffen. Demnach würde es keinerlei Rechtssicherheit für einen Hersteller oder privatwirtschaftlichen Anwender einer dieser Softwarearten geben. Im Fall einer Anzeige, beispielsweise durch ein konkurrierendes Unternehmen, würde eine Ermittlung ein-



geleitet und sämtliche Rechentechnik des betroffenen Unternehmens beschlagnahmt, um Beweismittel für ein Vorbereiten des Ausspähens und Abfangens von Daten zu sichern. Das betroffene Unternehmen wäre auch im Falle eines Freispruches seiner existenziellen Grundlagen beraubt und müsste den Betrieb einstellen.

Dienstleistungen im Bereich Computersicherheit, gleich welcher Art, sind Vertrauenssache. Kein Unternehmen würde Mitarbeiter einstellen oder Dienstleistungsunternehmen beauftragen, welche schon einmal auf Grund einer Computerstraftat aktenkundig geworden sind. Hierfür spielt es eine untergeordnete Rolle, ob es in dem betreffenden Fall zu einer rechtskräftigen Verurteilung kam.

Die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates bekräftigt, dass der Täter eine eigene oder fremde Computerstraftat in Aussicht genommen haben muss. Diese Einschränkung ist nicht im Gesetzestext verankert, obwohl dies gerade in Hinblick auf das obige Beispiel unbedingt erforderlich wäre. In der momentanen Fassung bietet der Gesetzestext keinerlei Rechtssicherheit.

Zum momentanen Zeitpunkt gehört Deutschland im Hochtechnologiebereich der Computersicherheit noch zu den führenden Nationen weltweit. Ein Inkrafttreten des vorliegenden § 202c E-StGB würde mit großer Sicherheit die Abwanderung der führenden Unternehmen zur Folge haben. Des Weiteren können Kunden in Deutschland die notwendigen Überprüfungsdienstleistungen nicht mehr einkaufen, da die Durchführung in vielen Fällen eine örtliche Präsenz voraussetzt, welche die Anbieter auf Grund der fehlenden Rechtssicherheit mit großer Wahrscheinlichkeit ablehnen müssen. Es kann auch nicht davon ausgegangen werden, dass die innerdeutsche Nachfrage etwas an dieser Entwicklung ändern wird, da die globale Nachfrage nach den entsprechenden Dienstleistungen im Hochqualifiziertenbereich deutlich größer ist als das Angebot und somit die wirtschaftlichen Auswirkungen für die abgewanderten Unternehmen minimal bleiben.

2.3.2 Fehlende Rechtssicherheit für Forschung

Computersicherheit lebt zum größten Teil von Forschung nicht industrieller Interessensgruppen. Hier sind vor allem akademische und private Interessensvereinigungen tätigt, welche mit Hilfe von neuen Angriffen die Sicherheit von Computersystemen kontinuierlich auf die Probe stellen, Lösungen für die identifizierten Probleme erarbeiten und beides kostenfrei öffentlich publizieren. Eine Abgrenzung, ob dadurch eine fremde Straftat in Aussicht genommen wurde ist unmöglich. Wenn es für Unternehmen schon schwierig wird nachzuweisen, dass ein Computerprogramm nicht in Vorbereitung auf das Ausspähen und Abfangen von Daten erstellt wurde, so ist dies für Privatpersonen und Interessensgruppen umso schwieriger. Eine Anzeige von einer beliebigen anderen Person hätte hier noch drastischere Auswirkungen auf das zukünftige Privat- und Berufsleben des betroffenen.

Die Publikation eines Sicherheitsproblems ist der Defacto Standard im Umgang mit einer solchen Entdeckung in der IT – Sicherheit. Dieses Vorgehen nennt man „Full Disclosure“. Kriminelle Gruppen versuchen seit nahezu zehn Jahren dieses Vorgehen zu unterbinden, da die öffentliche Darstellung eines Sicherheitsproblems alle Anwender, Administratoren und den Hersteller auf das Problem aufmerksam macht und damit die betroffenen Systeme in kürzester Zeit entsprechend geschützt werden. Ist die Information über das Sicherheitsproblem einmal öffentlich, ist sie für die krimi-

SABRE Labs GmbH
Wrangelstrasse 4
10997 Berlin
http://www.sabre-labs.com

nellen Organisationen wertlos. Solange allerdings das Problem nicht öffentlich ist, existiert kein Schutz und die kriminelle Organisation hat leichtes Spiel.

3 Empfehlung

In Anbetracht der Sachlage empfiehlt sich die Anwendung des Artikels 6, Abs. 3 der EU Cybercrime Convention:

„*Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.*“

Diese Stellungnahme geht mit Absicht ausschließlich auf den Absatz 2 des § 202c E-StGB ein, da die restlichen vorgeschlagenen Änderungen des Strafgesetzes vollständig ausreichen, um jede nur mögliche bekannte und zukünftig zu erwartende Computerstraftat rechtlich zu erfassen und zu ahnden. Die Streichung von § 202c Absatz 2 wäre keinerlei Beeinträchtigung.

Das Belassen von § 202c Absatz 2 hätte allerdings weit reichende wirtschaftliche und intellektuelle Folgen für das Gebiet der Computersicherheit in Deutschland. Kriminelle Personen und Vereinigungen könnten sich weiterhin jegliche Mittel über das Internet verschaffen, da keinerlei Einfuhrkontrollen möglich sind. Legitimen Unternehmen und Forschern würde allerdings jeder Handlungsspielraum genommen.

Anlage

DAS TROTZKOPF-PRINZIP, Matthias Spielkamp, BRAND EINS 01/07

DAS TROTZKOPF-PRINZIP

Die Bundesregierung will den Besitz von Programmen bestrafen, mit denen sich Schaden anrichten lässt. Dummerweise soll das auch für Sicherheitsfachleute gelten. Die IT-Branche kämpft in seltener Einigkeit gegen den Plan – vermutlich vergeblich.

Text: Matthias Spielkamp
Illustration: Xenia Fink

• Was täten Sie, wenn Sie einen Vorschlag machten, und alle, aber auch wirklich alle, die sich mit dem Thema auskennen, sagten Ihnen, dass es so nicht geht? Erst mal auf stur schalten und versuchen, den Ärger auszusitzen? Das wäre nur menschlich. Aber dann dächten Sie bestimmt noch mal nach – und änderten Ihre Meinung, wenn sich herausstellte: Das geht so wirklich nicht.

Nicht so das Bundesjustizministerium. Dort bleibt man lieber trotzig, auch wenn als Folge eine ganze Branche kriminalisiert wird. „Wenn das Gesetz so durchgeht, kommt das für mich einem Berufsverbot gleich“, sagt Felix Lindner zum Plan der Bundesregierung, den Paragrafen 202 des Strafgesetzbuches zu ändern und zu erweitern. Der Berliner Berater für IT-Sicherheit hat sich den Entwurf genau angesehen. Wer eine Straftat vorbereitet, heißt es dort, indem er „Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft“.

Völlig unsinnig sei diese Formulierung, sagt Lindner, denn sie bedeute, dass man all die Instrumente, die man einsetzt, um Systeme auf ihre Sicherheit zu testen, nicht mehr besitzen oder selbst programmieren darf, ohne sich strafbar zu machen. Denn es komme nicht darauf an, mit welchem Ziel jemand diese Hacker-Tools, wie die Branche derartige Software nennt, verwendet. Allein der Besitz ist strafbar. Hacker-Tools können zahlreiche Programme sein, die jeder Nutzer auf dem PC verwendet – vom Internet Explorer bis zur Firewall.

Deshalb ging ein Aufschrei durch die Branche, als der Gesetzesentwurf veröffentlicht wurde. „Das ist ein kurzes Gesetz“, sagt Volker Kitz, beim Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) zuständig für Telekommunikations- und Medienpolitik,

„aber ich habe selten eine so große Beunruhigung bei unseren Mitgliedsunternehmen gespürt." Das sind fast alle, die in der Branche Rang und Namen haben. Also hat der Verband der Regierung nahegelegt, doch bitte im Gesetz zu verankern, dass der Besitz oder Einsatz solcher Werkzeuge nur dann strafbar sein soll, wenn auch beabsichtigt ist, damit Schaden anzurichten.

In seltener Einigkeit fordern der Chaos Computer Club, der Verband der deutschen Internetwirtschaft und der Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik im Grunde das Gleiche. Wenn der Entwurf nicht geändert werde, so sagen sie, hätten alle, die sich mit Computersicherheit beschäftigen, ein ernstes Problem.

Denn es liegt in der Natur der Sache, dass man die Sicherheit von Computersystemen nur überprüfen kann, wenn man sie angreift. Das funktioniert in der Praxis zum Beispiel so, dass eine Firma den Auftrag bekommt zu überprüfen, ob es bei einem Webserver Lücken gibt, durch die Angreifer ins System eindringen könnten. Dazu setzt sie Programme ein, die genau das tun, was auch die Programme von echten Angreifern täten. Und damit würden sie sich künftig strafbar machen.

Nein, kontert Ulf Gerder, Sprecher des Bundesjustizministeriums. Denn in der Begründung des Gesetzesentwurfes steht, dass es auf den Vorsatz ankommt, mit einem Hacker-Tool eine Straftat begehen zu wollen. „Im Interesse, das Strafgesetzbuch schlank zu formulieren, wurde das nicht ins Gesetz aufgenommen, sondern in die Begründung", sagt Gerder.

Wie einen feuersicheren Safe bauen, wenn Flammenwerfer-Tests verboten sind?

Volker Kitz vom Bitkom sind schlanke Gesetze grundsätzlich sympathisch. Doch „was nicht explizit im Gesetz, sondern nur in der Begründung steht, kann einem heillos überlasteten Strafrichter leicht durchgehen. Der betreibt keine lange Quellenforschung, sondern schaut aufs Gesetz und sagt: Dieses im Prinzip legitime Vorgehen fällt auch darunter."

Nicht nur das, sagt Marco Gercke, Sprecher des Fachausschusses Strafrecht der Deutschen Gesellschaft für Recht und Informatik. „Der gesamte Entwurf erstaunt", sagt der Experte für Medienstrafrecht. „Wenn man sich die Literatur anschaut, die zur Begründung dient, dann stellt man fest, dass sie Mitte der neunziger Jahre aufhört. Viele der Probleme, die jetzt auf dem Tisch liegen, hätte man schon im Vorfeld sehen können, als der Entwurf entwickelt und begründet wurde." Nun werde der Selbstschutz der Unternehmen ausgehebelt, ohne dass der Gesetzgeber die Firmen schützen könne. „Hacker-Tools wird es weiter geben", sagt Gercke, denn diejenigen, die sie unerlaubt benutzen wollen, können sie sich jederzeit über das Internet besorgen.

In die Röhre schauen diejenigen, die sie für Forschung und Entwicklung einsetzen wollen, befürchtet Paul Frießem, vom Fraunhofer-Institut für Sichere Informationstechnologie in Sankt Augustin. „Unsere Studenten und Wissenschaftler schauen sich diese Werkzeuge an, um zu überprüfen, was man mit ihnen machen kann. Wenn ich mir Sicherheitsvorkehrungen ausdenke, die ich nicht überprüfen kann, habe ich ein Problem." Das sei ▸

ungefähr so, wie zu sagen, man solle einen feuersicheren Safe bauen, aber darf dann keinen Flammenwerfer verwenden, um ihn zu testen, weil der zu gefährlich und daher verboten sei.

Betroffen wären auch Vorzeige-Unternehmen wie die Essener Secunet Security Network AG mit mehr als 220 Mitarbeitern. Für das Auswärtige Amt hat die Firma das System entwickelt, mit der deutsche Botschaften im Ausland verschlüsselt mit der Berliner Zentrale kommunizieren können. Gerade derartige Anwendungen müssen auf alle erdenklichen Sicherheitslücken getestet werden. Der Unternehmenssprecher Kay Rathke findet die Diskussion, die um den Paragrafen 202 entbrannt ist, zwar sinnvoll und berechtigt, hofft aber, dass das „Gesetzgebungsverfahren so vernünftig ablaufen wird, dass man mit dem Ergebnis arbeiten kann". Er könne sich etwa vorstellen, dass es für Unternehmen wie Secunet Ausnahmegenehmigungen geben wird, die es ihnen erlauben, die Werkzeuge einzusetzen. „Das wäre dann wie bei den Betäubungsmitteln, die man zwar privat nicht besitzen darf, die aber zugelassene Ärzte eben doch in bestimmten Fällen einsetzen dürfen."

Der Fraunhofer-Forscher Frießem ist skeptischer. Derartige Ausnahmegenehmigungen seien in der Praxis nicht handhabbar: „Es geht um Werkzeuge, die der Netzwerkadministrator in jedem Unternehmen verwendet – denen kann man nicht allen eine Ausnahmegenehmigung geben." Genau, sagt auch Rolf vom Stein, Leiter der Abteilung Technische Sicherheit bei der TÜV Secure IT GmbH in Köln, einem der großen IT-Dienstleister, die in Deutschland Firmen wie die Bundesdruckerei nach internationalen Standards überprüfen und zertifizieren. „Vielleicht hätten wir als TÜV mit unserem Ruf eine gute Chance, eine Ausnahmegenehmigung zu bekommen. Aber wir empfehlen den Unternehmen sogar, ständig Sicherheits-Checks durch ihre eigenen IT-Leute machen zu lassen – die brauchten dann alle eine solche Ausnahmegenehmigung."

Überhaupt findet vom Stein kein gutes Wort für die Pläne des Bundesjustizministeriums: „Wenn der Entwurf so durchgeht, dann muss jeder meiner Techniker von drei Rechtsanwälten begleitet werden, die dafür sorgen, dass er nicht in Schwierigkeiten gerät." Er hat den Eindruck, dass sich die Bundesregierung von Experten beraten lasse, „die von dem Feld nur eine oberflächliche Ahnung haben". Das sei besonders ärgerlich, weil in der IT-Sicherheit in den vergangenen Jahren viel erreicht worden sei. „Früher hatten wir große Akzeptanzprobleme", erinnert sich vom Stein, „aber inzwischen kommen Banken mit fünf oder sechs Millionen Kunden zu uns, um ihre Systeme überprüfen zu lassen – mit diesem Gesetz würde das ganze Geschäft ad absurdum geführt." Das hätte auch zur Folge, dass der gesamten Volkswirtschaft Schäden durch unsichere Computersysteme entstünden.

Dass „die gesamte Sicherheitsszene pauschal kriminalisiert wird", befürchtet auch Frank Rosengart vom Chaos Computer Club. „Es ist unmöglich, abzugrenzen, um welche Programme es hier geht; im Grunde fallen sämtliche Bordmittel von Linux oder Windows unter diese Definition", beschreibt Rosengart den Stand der Technik: „Selbst Outlook, denn das kann genutzt werden, um Viren zu verbreiten."

Vor allem kleine Firmen und Freiberufler träfe das Gesetz hart, weil sie kaum von einem Tag auf den anderen etwas völlig anderes machen könnten, sagt IT-Berater Felix Lindner. Er habe sogar schon überlegt, den Unternehmensteil, der sich mit derartigen Überprüfungen beschäftigt, ins Ausland zu verlegen, wo andere Regelungen gelten. „Aber das nützt nichts", denn gerade kritische Systeme in Unternehmen seien nicht über das Internet erreichbar, weil sie nach außen abgeschottet sein müssen. „Wenn ich die überprüfen will, mache ich das mit dem Laptop in der entsprechenden Firma" – also dort, wo deutsches Recht und Gesetz gelten.

Bisher haben Firmen Sicherheits-Checks versäumt, künftig dürfen sie nicht mehr

Gerade deutsche Firmen in der Sicherheitsbranche haben einen Ruf zu verteidigen. So hat Microsoft sein neues Betriebssystem im Sommer von neun Unternehmen auf Lücken testen lassen. Fünf von ihnen kommen aus den USA, eines aus England, eines aus Indien und zwei aus Deutschland. Eines davon ist die Berliner Firma Code Blau. Ihr Gründer Felix von Leitner sagt, dass er sich zwar überlegen müsste, wie er weitermacht, wenn das Gesetz so durchgeht wie angekündigt. Aber die wirtschaftliche Situation sei nicht das größte Problem: „Wir machen auch sogenannte Quellcode-Audits, das heißt, wir analysieren den Programmcode", so von Leitner. „Das könnten wir weiterhin tun, und programmieren können wir auch."

Viel wichtiger sei, dass durch das Gesetz den Kunden das „einzige Schwert, das sie haben, um auf die Anbieter von Software Einfluss zu nehmen, aus der Hand geschlagen wird", so von Leitner – nämlich selbst zu überprüfen, ob deren Systeme sicher seien. „Die ganze Hacker-Kultur hat sich entwickelt, weil Firmen ihre Sicherheitslücken nicht schließen." Der Weltkonzern Oracle etwa veröffentliche nur alle drei Monate neue Updates für seine Software, manche bekannten Schwachstellen seien seit Jahren nicht beseitigt. Darüber hinaus gebe es genug Anwendungen, bei denen alle ein Recht darauf hätten zu erfahren, ob sie sicher seien. „Die neuesten Reisepässe haben Smart Cards, und ich kann nicht herausfinden, ob die sicher sind, wenn ich keine Hacker-Tools verwenden darf", sagt von Leitner.

„Beim Paragrafen 202 ist einfach keine Rechtssicherheit gegeben", ist auch der Jurist Gercke überzeugt. Das Gesetz müsse so ergänzt werden, dass der legitime Einsatz derartiger Programme explizit erlaubt wird. „Aber in letzter Zeit", fasst Gercke seinen Eindruck von diesem und anderen Gesetzgebungsverfahren zusammen, „zeigt sich der Gesetzgeber oft beratungsresistent, bisweilen sogar arrogant."

Und bei den Hacker-Tools? Nachdem auch der Bundesrat die Kritik der Interessenverbände, Unternehmen, Hacker und Forscher in den wichtigen Punkten übernommen und den Gesetzgeber aufgefordert hatte, den Entwurf zu ändern, veröffentlichte das Justizministerium Anfang Dezember seine Erwiderung. Darin heißt es: „Die Befürchtung, dass auch der gutwillige Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen von § 202c StGB-E erfasst werden könnte, ist nicht begründet." ▬