Die Überkriminalisierung der IT-Sicherheitsbranche in Deutschland

*Textbeitrag von Jörg Tauss. In: it-Information Technology. 1/2008. S. 70-73**

* *mit freundlicher Genehmigung des Oldenbourg Wissenschaftsverlages*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat es nicht leicht. Als zentraler IT-Sicherheitsdienstleister des Bundes hat es sich zum Ziel gesetzt und hat zugleich den gesetzlichen Auftrag, die IT-Sicherheit in Deutschland voran zubringen. Mit Handlungsrichtlinien und Grundlageninformationen wendet sich das BSI an Hersteller und Nutzer von Informationstechnik und überzeugt seit Jahren durch ein hohes Maß an Fachkompetenz. Die Bonner Behörde gilt daher auch bei IT-Sicherheitsexperten zu Recht, als vorbildliche, kompetent, flexibel und zuverlässig arbeitende Bundesbehörde. Bisher. Denn trotz dieser positiven Attribute sieht sich das Bundesamt für Sicherheit in der Informationstechnik nun mit einer Strafanzeige konfrontiert. Mit der Bereitstellung der BOSS-Software-Suite auf der eigenen Web-Seite soll das BSI gegen den seit dem 10. August 2007 geltenden §202c im Strafgesetzbuch (StGB) verstoßen haben. Das BSI eine kriminelle Vereinigung?

Hintergrund

Die Bundesregierung hat im Herbst 2006 den Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vorgelegt. Darin sollten das Übereinkommen des Europarats über Computerkriminalität und der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme umgesetzt werden. Ziel des Europarat-Übereinkommens, der so genannten Cybercrime-Konvention, ist die Schaffung eines europaweiten strafrechtlichen Mindeststandards, um so Computersysteme und -daten zu schützen und gleichzeitig ihrem Missbrauch entgegen zu wirken. Vorgesehen waren im Entwurf der Bundesregierung eine Änderung und Ergänzung des §202a und eine Einfügung der §§202b und 202c StGB. Das mit dem Gesetzentwurf verfolgte originäre Ziel wurde von einem Großteil der Fraktionen im Deutschen Bundestag, aber auch von Seiten betroffener Verbände, Unternehmen und Organisationen prinzipiell begrüßt. Angesichts der sich rasch verändernden Informations- und Telekommunikationstechnologien in den vergangenen Jahren war eine Verbesserung des geltenden Computerstrafrechts dringend geboten.

Aus forschungs- und medienpolitischer Sicht war der vorgelegte Entwurf in seiner konkreten Ausgestaltung allerdings in keinster Weise geeignet, die beabsichtigte Verbesserung herzustellen. Ganz im Gegenteil, gab es doch bereits kurz nach Bekanntwerden des Gesetzentwurfes und insbesondere bezogen auf den neuen §202c - zu Recht - massive Kritik, da weitreichende und negative Auswirkungen für die IT-Sicherheit, die IT-Sicherheitsforschung und die Informations- und Kommunikationsbranche in Deutschland befürchtet wurden. Dargelegt und bestätigt wurde die Kritik sowohl in einem Expertengespräch des Unterausschusses Neue Medien des Deutschen Bundestages, als auch in der Sachverständigenanhörung des federführenden Rechtsausschusses des Deutschen Bundestages; selten war eine so breite Übereinstimmung in der Sache zwischen den Experten aus der Wissenschaft und den Vertretern der betroffenen Branchen zu sehen. Nahezu einhellig war die Meinung der Experten, dass der Gesetzentwurf zwar in die richtige Richtung ziele, zugleich aller-

dings verschiedene handwerkliche Mängel aufwies, die mindestens eine Klarstellung respektive Korrektur, insbesondere des objektiven Tatbestandes, verlangten. Schon mit marginalen Änderungen hätte auch nach Auffassung namhafter Rechts- und IT-Experten eine deutliche Verbesserung erreicht werden können. Entsprechende Vorschläge zur Änderung des Gesetzentwurfes der Bundesregierung für ein Strafrechtsänderungsgesetz lagen dem federführenden Rechtsauschuss vor, fanden jedoch keine Berücksichtigung.

Problematisch war vor allem die Einfügung des § 202c StGB, mit dem typische Vorbereitungshandlungen unter Strafe gestellt werden, was dem Strafrecht - bis auf wenige Ausnahmen - sonst fremd ist. Dieser Regelungsvorschlag war vor allem deshalb problematisch, weil entsprechende Programme und Tools nicht nach ihrer Einsatzart, sondern vielmehr nach ihrem Aufbau definiert werden und so eine Unterscheidung in Programme, die zur Begehung von Straftaten hergestellt werden, und solche, die ausschließlich für legale Zwecke hergestellt werden, schlichtweg nicht möglich ist. Lediglich in der Verwendung lassen sie sich unterscheiden. Eine vom Gesetzentwurf bezweckte Unterscheidung in „gute“ und „schlechte“ Programme ist allein schon deshalb nicht möglich, weil die benannten Programme einen identischen Aufbau haben - dies gehört zum Basiswissen im Bereich der IuK-Technologie.

Zusammenfassend lässt sich sagen, dass der §202c weit über die zugrundeliegende Cybercrime-Konvention hinausgeht, in welcher nur die vorsätzliche und unbefugte Nutzung der Tools strafbar ist, nicht aber die Vorbereitungshandlung und welche somit Punkt zwei der Konvention sogar diametral entgegen steht. Der in §202c gewählte Wortlaut führt zu einer Kriminalisierung der heute millionenfach verwendeten Programme, welche auch für Testzwecke und das Entdecken von Sicherheitslücken in IT-Systemen notwendig sind – Programme, die selbst das Bundesamt für Sicherheit in der Informationstechnik zu jenem Zeitpunkt verwendet und zum Download angeboten hat. Eine komplette Streichung des in meinen Augen mehrdeutigen und praxisfremden §202c, mindestens aber eine Präzisierung oder aber marginale Änderungen wären notwendig gewesen und wurde so auch gefordert bzw. eingebracht.

Trotz allem: Nach insgesamt als völlig unzureichend zu bezeichnenden Beratungen in den Gremien des Deutschen Bundestages und trotz der massiven Kritik aus Expertenkreisen wurde das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität am 25. Mai 2007 vom Deutschen Bundstag verabschiedet. Da das Gesetz schlichtweg nicht verabschiedungsreif war, habe ich erstmalig seit 1994 in einer für mich wichtigen Frage in 2./3. Lesung einem Gesetzentwurf meine Zustimmung verweigert und gegen meine eigene Fraktion gestimmt.

Dass das Gesetz in seiner Form nicht verabschiedungsreif war, schien nun offenbar auch dem federführenden Rechtsausschuss bekannt zu sein, denn in der Beschlussempfehlung des Gesetzentwurfes heißt es wörtlich: „Der Gesetzgeber wird die Auswirkungen der neuen Strafvorschriften genau zu beobachten haben. Sollten doch Programmentwickler und Firmen, die nicht aus krimineller Energie heraus handeln, durch diese neuen Strafvorschriften in Ermittlungsverfahren einbezogen werden, wird auf solche Entwicklungen zeitnah reagiert werden müssen.“ Vor diesem Hintergrund ist es aber absolut nicht nachvollziehbar, warum sämtliche Änderungsvorschläge im parlamentarischen Verfahren, die eben dies ausschließen sollten, schlichtweg ignoriert wurden. Gesetze nach dem Motto „trial and error“ sind nicht akzeptabel - zumal dann, wenn damit in Konsequenz ganze Berufsbranchen wie Sys-

temadministratoren, Software-Händler und IT-Sicherheitsexperten ohne jeden vernünftigen Grund und ohne jede Notwendigkeit kriminalisiert werden.

Konsequenzen

Die Reaktionen aus der IT-Sicherheitsbranche, der Wissenschaft, aus den Interessenverbände und den betroffenen Unternehmen waren nach der Verabschiedung des Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität durch den Bundestag und Bundesrat eindeutig: Kopfschütteln und Verunsicherung.
Zu Recht schütteln IT-Experten mit dem Kopf über das Gesetz, welches in dieser Form vermeidbar gewesen wäre. Weitaus dramatischer als das Kopfschütteln der gesamten IT- Sicherheitsbranche ist allerdings die durch das Gesetz entstandene Verunsicherung innerhalb einer gesamten Berufsbranche. Auf der einen Seite soll sie für die Sicherheit und Stabilität von Netzwerken und informationstechnischen Systemen sorgen, auf der anderen Seite wird ihr das originäre Handwerkszeug genommen, weil es sich unter Umständen auch für illegale Aktionen nutzen lässt. Es handelt sich dabei um unverzichtbare Tools, die in Unternehmen, Behörden und von Privaten millionenfach zur Aufdeckung von Sicherheitslücken in IT-Systemen verwendet werden.

Konsequenterweise verlagern daher bereits die ersten Unternehmen, die sich mit dem Entwickeln von Sicherheitsprogrammen und Sicherheitstools befassen, ihre Server ins Ausland, beenden laufende Projekte oder schließen gar ihre Internetauftritte.

Das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität gefährdet auf massive Art und Weise den bisher international als sehr gut bezeichneten IT-Standort Deutschland und konterkariert überdies die Bemühungen der Bundesregierung geradezu, wo beispielsweise im Rahmen des Sicherheitsforschungsprogramms sehr viel Geld für die IT-Sicherheitsforschung ausgeben wird. Richtigerweise hat man auf Seiten der Bundesregierung erkannt, dass IT-Sicherheit in unserer heutigen Informations- und Wissensgesellschaft zunehmend die Grundlage für nahezu jegliches wirtschaftliches Wachstum bildet. Das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität führt dies allerdings ad absurdum, da eine klare Gefährdung und Benachteiligung des IT-Standortes Deutschland gegenüber anderen Ländern droht und damit verbunden der Verlust von Arbeitsplätzen. Insbesondere weil so vorhandenes Know-how in Deutschland gefährdet wird, da der Entwicklung von Sicherheitsprogrammen die mögliche Strafverfolgung entgegensteht. Dies ist eine Gefahr für den gesamten Wirtschaftszweig und führt überdies zu Problemen in der Nachwuchsrekrutierung. Zumal der Normwortlaut so uneindeutig ist, dass sogar jegliche Lehre, Forschung und Entwicklung und auch der einfache Gedankenaustausch zu Tools und Applikationen an Universitäten und Fachhochschulen mit diesem Paragrafen unter Strafe gestellt werden könnte.

Um es klar zu sagen: Es geht nicht um die Bagatellisierung oder Entkriminalisierung von Straftaten, sondern es geht um die Sicherstellung von IT-Sicherheit und IT-Sicherheitsforschung in Deutschland. Das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität verhindert eine solche Sicherstellung und schwächt den IT-Standort Deutschland. Die Folge: Rechtsunsicherheit für Administratoren, Entwickler, aber eben auch für den normalen Anwender. Überdies wird der Wirtschaft, aber auch dem normalen Bürger, mit dem engen Normlaut systematisch die Möglichkeit genommen, ihre Systeme adäquat auf Sicherheit zu überprüfen. Dies

öffnet nicht nur der internetbasierten Kleinkriminalität Tür und Tor, sondern erschwert den notwendigen IT-Schutz deutscher Unternehmen vor international agierenden Wirtschaftskriminellen, die eben nicht vor deutschen Strafgesetzbüchern Halt machen.

In diesem Kontext ist auch auf die Debatte um die so genannte Online-Durchsuchung einzugehen. Wie sie den Medienberichten der letzten Wochen und Monate entnehmen konnten, sind die SPD und die SPD-Bundestagsfraktion beim Thema Online-Durchsuchung sehr skeptisch. Bevor man ein solches heimliches Ermittlungsinstrument einführt, mit dem tief in die Privatsphäre der Nutzerinnen und Nutzer und möglicherweise auch in den Kernbereich der privaten Lebensführung eingegriffen wird, müssen auch die technischen Möglichkeiten, wie auch deren Grenzen, deren Folgen und die rechtlichen – insbesondere die verfassungsrechtlichen – Voraussetzungen geklärt und die Notwendigkeit eines solchen Instrumentes ausreichend dargelegt werden. Gerade wegen der technischen und rechtlichen Probleme einer Online-Durchsuchung wurde seitens des BMJ und seitens der Arbeitsgruppen für Bildung und Forschung sowie Kultur und Medien sehr umfangreiche Fragenkataloge vorgelegt und in der Zwischenzeit vom BMI formal „beantwortet". Dennoch bleiben zahlreiche Fragen unbeantwortet oder werfen sogar weitere Fragen auf und die SPD-Bundestagsfraktion besteht auf Klärung dieser Fragen. Um nur die wichtigsten zu nennen: Es muss zunächst die tatsächliche Notwendigkeit und verfassungsrechtliche Zulässigkeit eines solchen Instrumentes dargelegt und insbesondere geklärt werden, wie den datenschutz- und persönlichkeitsrechtlichen Grundsätzen entsprochen und der Kernbereich der privaten Lebensführung gewahrt bleiben soll, wie ihn das Verfassungsgericht beim großen Lauschangriff vorgegeben hat. Daneben muss es Sicherungen zum Ausgleich des verdeckten Charakters der Ermittlungsmaßnahme geben, um die Rechte der Betroffenen zu wahren. Geklärt werden muss zudem der gerichtsfeste Beweiswert dieser mittels der Online-Durchsuchung gewonnenen Erkenntnisse. Sichergestellt werden muss darüber hinaus, dass dieses Instrument nicht durch Dritte missbraucht und die Verwundbarkeit der Informations- und Kommunikationsinfrastruktur erhöht bzw. die Akzeptanz der IuK-Technologie gefährdet. Zu befürchten ist durchaus, dass unsichere IT-Systeme neue Formen von Kriminalität und Terrorismus hervorbringen könnten (Eindringen in kritische Infrastrukturen, Bankgeschäfte etc.). Auch muss geklärt werden, wie der Schutz Unbeteiligter gewährleistet wird, nicht unbeabsichtigt von einer Online-Durchsuchung erfasst zu werden.

Womit wir am Ende dieses Beitrages wieder beim BSI wären, welches sich nun mit einer Strafanzeige konfrontiert sieht. Während die Änderungen des Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität IT-Sicherheits-Tools und die IT-Sicherheitsforschung kriminalisiert und massiv gefährdet, setzt die Online-Durchsuchung ein mehr oder minder „unsicheres" Netz voraus. Damit einher geht eine Umwertung der bisherigen Sicherheitspolitik in Deutschland. Die Sicherheitsbehörden machen das Netz nicht sicherer, sondern im Gegenteil: Es gibt ein staatliches Interesse, „Hintertüren" und Sicherheitslecks in Betriebs- und Anwendungssystemen zu nutzen oder sogar „einzubauen". Hinzu kommt natürlich die Tatsache, dass - wenn die deutschen Sicherheitsbehörden heimlich auf Rechner zugreifen können - dies dann auch Dienste anderer Staaten können. Eine in diesem Zusammenhang sehr zentrale Frage stellt derzeit niemand: Welche Rolle spielt dann das BSI und wie möchte das BSI der abzusehenden Vertrauenskrise, der sich auch eine erneute BSI-Debatte anschließen wird, begegnen? Die Akzeptanz und das Vertrauen in die Arbeit

des Bundesamtes für Sicherheit in der Informationstechnik ist jedoch eine zentrale Voraussetzung, die IT-Sicherheit und die IT-Sicherheitsforschung in Deutschland voranzubringen.