EICAR Legal Advisory Board veröffentlicht Stellungnahme zur Strafbarkeit beim Umgang mit IT-Sicherheitstools

Erstes Arbeitsergebnis des neu gegründeten EICAR-Fachbereichs beschäftigt sich mit dem aktuell viel diskutierten § 202c StGB

München, 22. Oktober 2007 – Die *European Expert Group for IT Security (EICAR)* stellt sein Positionspapier zur Strafbarkeit beim Umgang mit IT-Sicherheitstools in Zusammenhang mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität der Öffentlichkeit vor. Kernthese des Papiers ist, dass es keine klare Definition seitens des Gesetzgebers darüber gibt, welcher Einsatz von Hacker-Werkzeugen durch IT-Security Experten und Unternehmen eine strafbare Handlung darstellt. Der Bundestag hat es versäumt, vom Europarat in der Cybercrime Convention vorgesehene Ausnahmen eindeutig ins deutsche Strafrecht umzusetzen. Es besteht demnach in einigen Teilen erhebliche Rechtsunsicherheit. Das Positionspapier kann unter www.eicar.org heruntergeladen werden.

Preisgekrönter Autor verfasst sachliche Einschätzung zu viel diskutiertem Paragraphen

„Als Autor des Positionspapiers konnten wir Dennis Jlussi gewinnen. Er ist aktueller Träger des Nachwuchspreises der deutschen Stiftung für Recht und Informatik und hat die Kommentierung im Rahmen einer Projektarbeit mit seinem Kollegen Christian Hawellek erstellt", kommentiert Prof. Dr. Nikolaus Forgo, Vorsitzender des EICAR Legal Advisory Boards.
Als Kernthese geht aus dem Positionspapier hervor, dass der deutsche Gesetzgeber es nicht vermocht hat, entsprechend der Cybercrime Convention gutartige Tätigkeiten im Rahmen der IT-Sicherheit klar von den Straftatbeständen auszunehmen. Das gilt speziell dann, wenn sich IT-Sicherheitsexperten oder Entwickler mit Viren auseinanderzusetzen, um entsprechende Sicherheitssoftware zu programmieren.
In diesem Zusammenhang besteht in Teilen Rechtsunsicherheit.

Einführung des §202c StGB sorgt für Diskussion

Die Einführung des § 202c StGB durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität[1] (41. StrÄndG) ist in den Medien und von betroffenen Fachkreisen scharf kritisiert worden; Maßnahmen der IT-Sicherheit würden kriminalisiert und auch nach allgemeiner Anschauung gutartige Anwender von Hackertools seien „von der Gnade des Richters" abhängig.[2]

Das Gesetz ändert und ergänzt die Strafrechtsbestimmungen über Computerkriminalität: Beim Ausspähen von Daten (§ 202a StGB) kommt es nicht mehr auf einen Erfolg an, das heißt, es ist nunmehr unerheblich, ob der Täter tatsächlich Daten erlangt, es genügt die Möglichkeit des Zugangs zu Daten. Der Tatbestand des Abfangens von Daten (§ 202b StGB) ist neu geschaffen und der der Computersabotage (§ 303b StGB) ausgeweitet worden. Als Tätigkeiten, die unter § 202c StGB fallen könnten, kommen insbesondere die Beschaffung, Erstellung, Anpassung und Verwendung von Software in Frage, und zwar einerseits für die IT-Sicherheit designte Software zur Schwachstellenanalyse (z. B. AppScan, GFI Languard, Nessus). Solche Software versucht (unter anderem), Sicherheitslücken aufzuspüren, indem bestimmte potenziell schädliche Werte an das zu testende System übergeben und sodann Reaktionsmuster („Signaturen") ausgewertet werden. Andererseits kommt aber auch Schadsoftware (Viren, Trojaner, Würmer Exploits etc.) in Frage, die beschafft und angewendet wird, um zu testen, ob Computersysteme für bestimmte Angriffe anfällig sind oder ob die Systeme durch aktuelle Patches und Sicherheitssoftware (z. B. Virenscanner) ausreichend und wirksam geschützt sind.

Keine eindeutige Rechtslage – dennoch keine Panik angesagt

„Durch Beachtung einiger weniger Vorsichtmaßnahmen kann das Strafbarkeitsrisiko minimiert werden", meint der Autor Dennis Jlussi. „Es ist also keine Panik angesagt. Die Rechtslage ist zwar nicht ganz eindeutig – eine höchstrichterliche oder obergerichtliche Rechtssprechung liegt auch nicht vor." Dennoch ist davon auszugehen, dass bei Beachtung geeigneter Maßnahmen keine strafbaren Handlungen vorliegen.

[1] BGBl I Nr. 38/2007, S. 1786 ff.
[2] *Lischka,* Gesetz kriminalisiert Programmierer, Spiegel Online, http://www.spiegel.de/netzwelt/web/0,1518,492932,00.html.

EICAR Legal Advisory Board beschäftigt sich mit neutralen Rechtseinschätzungen

Das EICAR Legal Advisory Board ist ein neu gegründeter Fachbereich unter dem Dach der europäischen Sicherheitsorganisation. Als Vorsitzender des Boards konnte der renommierte IT-Rechtsexperte Prof. Dr. Nikolaus Forgo gewonnen werden. Das EICAR Legal Advisory Board wird sich in Zukunft mit aktuellen Rechtsfragen, die in einem Zusammenhang mit Informationssicherheit stehen, auseinander setzen. Darüber hinaus steht das Board als neutrale Informationsstelle für IT-Rechtsfragen zur Verfügung. Hierbei soll insbesondere das neue EICAR Forum (https://secure.eicar.org/forum/) als interaktive Kommunikationsplattform unterstützen.

Kurzprofil EICAR: Die EICAR wurde 1991 als eingetragener Verein in Deutschland gegründet. Zunächst mit dem Ziel, Know-how im Bereich der Antivirenforschung zu bündeln, gilt die EICAR mittlerweile als anerkanntes IT-Security Expertennetzwerk. Das Institut versteht sich als Plattform für den Informationsaustausch für alle Sicherheitsexperten, die in den Bereichen Forschung und Entwicklung, Implementierung sowie Management tätig sind. Hierdurch soll die globale Zusammenarbeit im Bereich der Computersicherheit gefördert werden. Ziel des Instituts ist es, Lösungen und Präventivmaßnahmen gegenüber allen Arten der Computerkriminalität, wie z.B. das Schreiben und Verbreiten von Computer-Viren, Betrug sowie das Ausspähen von personenbezogenen Daten, zu entwickeln. Dabei arbeitet das Institut sowohl sehr eng mit Unternehmen, politischen Organisationen oder universitären Einrichtungen als auch Medien, Technik- und Rechtsexperten zusammen.

Kontakt für Presseanfragen:

Manuel Hüttl
EICAR Director Business Development
E-Mail: dirbus@eicar.org
Telefon: 089-62817529

Eddy Willems
EICAR Director Information and Press
E-Mail: press@eicar.org
Telefon: + 32 (0)479-985432