EICAR Legal Advisory Board veröffentlicht Stellungnahme zur strafrechtlichen Relevanz von IT-Sicherheitsaudits

Neu gegründeter EICAR-Fachbereichs beleuchtet Sicherheitsüberprüfungen vor dem Hintergrund des neuen Computerstrafrechts

München, 16. April 2008 – Die *European Expert Group for IT Security (EICAR)* stellt ihr Positionspapier zur strafrechtlichen Relevanz von IT-Sicherheitsaudits der Öffentlichkeit vor. Kernthese des Papiers ist, dass die überwiegende Zahl der IT-Sicherheitsüberprüfungen jeweils nur dann zulässig sind, wenn zuvor durch den Rechtsgutsträger eine Gestattung der entsprechenden Tätigkeiten im vorzunehmenden Umfang erfolgt. Der Autor Christian Hawellek hat das Papier im Rahmen einer Projektarbeit am Lehrstuhl für Rechtsinformatik der Universität Hannover für das Legal Advisory Board der EICAR erstellt.

Die Durchführung von IT-Sicherheitsüberprüfungen ist essentielle Voraussetzung für die Gewährleistung von Informationsschutz, Daten- und Netwerksicherheit im eigenen Unternehmen. Sie liegt damit nicht nur im ureigenen wirtschaftlichen Interesse, sondern ist zumindest für Aktiengesellschaften aufgrund § 91 II AktG auch rechtlich geboten. Die rechtlichen Rahmenbedingungen sind allerdings, gerade mit Blick auf das im Sommer 2007 erheblich ausgeweitete deutsche Computerstrafrecht, alles andere als trivial und erschließen sich nicht etwa durch einfachen Blick in das Gesetz. Ein hohes Maß an Rechtssicherheit für die beteiligten Fachkreise ist aber Grundvoraussetzung für die Durchführung effektiver Sicherheitsaudits.

Generell gestattet sind nach neuer Rechtslage ausschließlich rein passive Scans nach Sicherheitslücken, die ohne jegliche weitere Penetration der gescannten Systeme erfolgen. Jede darüber hinausgehende Überprüfung hingegen fällt üblicherweise in den Anwendungsbereich des Computerstrafrechts und ist damit erst bei Vorliegen weiterer besonderer Voraussetzungen zulässig. So stellt das Ausnutzen von Sicherheitslücken zur Erlangung des Zugangs zu Daten oder Systemen – sei es mit Hilfe der erweiterten Funktionen von Scan-Software wie AppScan, der Nutzung eigener oder fremder Exploits, XSS, SQL-Injections oder

aber Passwortcracks – ein Ausspähen von Daten i. S. d. § 202a StGB dar. Handlungen zur Überprüfung der Leistungsfähigkeit von Antivirus- und Antispy-Programmen können in den Anwendungsbereich des § 303a StGB (Datenveränderung) fallen, der Einsatz sog. „Sniffer“ schließlich ist ein klassischer Fall des Abfangens von Daten (§ 202b StGB).

Zwingende Voraussetzung für die strafrechtliche Zulässigkeit der vorgenannten Handlungen ist damit die Gestattung durch den jeweiligen Rechtsgutsträger, soweit nicht sonstige Rechtfertigungsgründe eingreifen. Problematisch ist dabei vor allem die exakte Bestimmung des jeweils geschützten Personenkreises, insbesondere wenn Informationssysteme in bestimmtem Umfang auch privat genutzt werden dürfen. Sind ausschließlich Rechtsgüter des überprüften Unternehmens betroffen, ist die Genehmigung durch dessen rechtlichen Vertreter zu erteilen, wobei dieses Recht im Rahmen der Unternehmensorganisation an nach geordnete Stellen delegiert werden kann. Die Einverständniserklärung ist dabei hinreichend umfänglich und präzise zu formulieren, generell gilt: je stärker der Eingriff und je größer das Risiko, desto höher sind die hieran zu stellenden Anforderungen.

Sind auch Rechtsgüter Dritter betroffen, so sind Eingriffe nur zulässig, wenn entweder auch deren jeweilige Zustimmung vorliegt – ggf. auch in Form entsprechender Betriebsvereinbarungen mit den Arbeitnehmern –, oder aber spezielle Rechtfertigungsgründe eingreifen. So ist etwa der Einsatz von „Sniffern“, soweit zur Sicherstellung der Netzwerkfunktionalität erforderlich, aufgrund § 88 III TKG gerechtfertigt, das Löschen privater Daten auf Unternehmenssystemen schließlich kann bei entsprechender Gefahrenlage als Notstandshandlung zulässig sein. Werden ansonsten die Überprüfungen im Rahmen der rechtswirksamen Gestattung durchgeführt, ist auch nach neuer Rechtslage ein hohes Maß an Rechtssicherheit möglich.

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