

Ulrich Emmert

Hackertools im Visier der Justiz

c't 02/2002, S. 76

Bisher ist in Deutschland weder der Besitz noch die Verbreitung von Programmen strafbar, die für Einbrüche in Computer genutzt werden können. Doch das könnte sich bald ändern. Am 4. Juli 2001 beschloss das Kabinett den Entwurf des so genannten Zugangskontrolldiensteschutzgesetzes (ZKDSG), welches für 'Umgehungsvorrichtungen' zur 'unerlaubten Nutzung eines zugangskontrollierten Dienstes' in bisher kaum dagewesener Schärfe bereits Besitz, Einrichtung, Wartung und Austausch verbietet, sofern diese als 'gewerbsmäßig' zu bezeichnen sind.

Das eigentliche Ziel der Gesetzesvorlage ist der Schutz von kostenpflichtigen Internet- und PayTV-Angeboten. Doch nach dem Gesetzeswortlaut kann davon auch der Besitz und die Verwendung von Passwort-Crackern oder von Kryptoanalysesoftware betroffen sein, die zum Testen von Firmennetzen eingesetzt werden. Firmen, die im Kundenauftrag Sicherheitstests durchführen, nutzen die gleichen Tools zur Überwindung von technischen Schranken wie die Hacker selbst. Der bloße Besitz solcher Tools ist daher wertneutral und bisher nur bei böswilliger Verwendung strafrechtlich relevant.

Sollten auch die Verbreitung und Besitz solcher Software in der Rechtspraxis verfolgt werden, dann wird dies mehr Schaden als Nutzen hervorbringen. Ein Cracker wird sich von Gesetzen kaum davon abhalten lassen, sich entsprechende Tools zu besorgen oder weiterzuverbreiten. Der gesetzestreue Administrator oder Security-Consultant sieht sich dagegen in seiner Arbeit behindert. Schon der Besitz oder die Wartung solcher Tools kann mit einem Bußgeld bis zu fünfzigtausend Euro belegt werden. Die Eingrenzung 'zu gewerbsmäßigen Zwecken', die den Privatmann vor einer Strafverfolgung schützt, hilft dem Security-Consultant leider nichts, da auch er mit den Tools Geld verdienen möchte.

Das Gesetz ergeht aufgrund einer europäischen Richtlinie, die angemessene Maßnahmen fordert, die die Umgehung von Zugangskontrolldiensten verhindern. Das scharfe Schwert des Strafrechts wird von der Richtlinie ausdrücklich nicht gefordert, sondern sie überlässt die Auswahl der gesetzgeberischen Mittel den Mitgliedsstaaten. Wenn Deutschland schon eine Strafbarkeit für notwendig erachtet, sollte doch wenigstens versucht werden, die Konturen dieses Straftatbestands nochmals zu schärfen, um schädliche Effekte auszuschließen. Als Beispiel könnte das mittlerweile unterzeichnete Cybercrime-Abkommen dienen, das Bestrafung des Missbrauchs von Einrichtungen für Hackerzwecke an die Absicht bindet, damit kriminelle Zwecke zu verfolgen.

Ulrich Emmert ist Rechtsanwalt und unter www.kanzlei.de zu erreichen.