KES, Zeitschrift für IT-SIcherheit, Secumedia Verlag, Ausgabe 5/2005
Ulrich Emmert

Strafbare Sicherheits-Tools?

Langsam wird es immer enger für Hacker und Premiere-Schwarzseher in Deutschland: Nicht nur die Strafbarkeit des „Schwarzsehens“ und das Abschalten der sogenannten „Monitoring-Schlüssel“ für Händler macht den Premiere-World-Piraten zu schaffen, auch das Anbieten entsprechender Crack-Software für analoge oder digitale Zugänge im Internet ist seit 23. März mit dem Zugangskontrolldiensteschutzgesetz unter Strafe gestellt worden. Das Gesetz verliert vielleicht schon kurz nach seinem Inkrafttreten den größten Teil seines geplanten Anwendungsbereichs, wenn im Rahmen der Kirch-Insolvenz der hoch defizitäre Pay-TV-Sender Premiere World eingestellt werden sollte.

Dies ist aber nur ein Baustein in den Bemühungen der europäischen Staaten, der stark ansteigenden „Cyberkriminalität“ Herr zu werden. Bisher nutzen die Hacker die fehlende internationale Harmonisierung der Strafrechtsvorschriften perfekt aus. In den relativ liberalen Niederlanden konnten Musiktauschbörsen, Raubkopie- und Pornoanbieter noch bis vor kurzem weitgehend unbehelligt ihrer Tätigkeit nachgehen. Staaten wie Togo vergeben z.B. Domains, die nirgendwo einem Besitzer zugeordnet werden können und daher häufig zu illegalen Zwecken missbraucht werden.

Cybercrime-Abkommen des Europarates

Diesen Problemen will man zumindest im europäischen Rahmen zu Leibe rücken. Am 9. November 2001 ist der 27. Diskussionsentwurf des Cybercrime-Abkommens des Europarats endgültig abgesegnet worden. Seit 23. November 2001 signieren die Staaten das Abkommen und ratifizieren es anschließend durch die Parlamente. Es enthält Vereinbarungen zur Überwachung und Verfolgung von Straftaten im und über das Internet. Dabei sollen sowohl die strafrechtlichen Grundlagen des ”Hacker-Strafrechts“ als auch die Überwachungs- und Verfolgungsmaßnahmen vereinheitlicht und die internationale Zusammenarbeit verbessert werden.

Strafbarkeitslücken in Deutschland

Die Mitgliedsstaaten verpflichten sich, bei der Verfolgung von Hackern einen ganzen Katalog von Verhaltensweisen unter Strafe zu stellen. In vielen Ländern, auch unter den 41 Mitgliedsstaaten des Europarats, fehlen einzelne oder auch eine ganze Reihe von Strafvorschriften, um die Cyberkriminalität wirksam bekämpfen zu können. Im Bereich Hacking sollen der unerlaubte Zugriff auf Rechnersysteme, das Abhören und Sniffen von Daten, Störung oder Veränderung der Kommunikation, Störung von Computersystemen und der Missbrauch von Geräten und Programmen (auch der Besitz mit der Absicht des Missbrauchs) sowie Fälschung von Daten und Betrug durch Datenveränderung oder Störung von Computern in allen Mitgliedsstaaten unter Strafe gestellt werden. Beim Ausspähen von Daten wird den Mitgliedsstaaten die Möglichkeit eingeräumt, die Überwindung von technischen Schranken, eine besondere Absicht des Ausspähens oder das Ausspähen über vernetzte Computer zur Voraussetzung der Strafbarkeit zu machen. Demnach entspricht das deutsche Recht den Anforderungen der Konvention, da hier eine Überwindung einer technischen Hürde und das tatsächliche Ausspähen von Daten zur Strafbarkeit erforderlich sind. In Deutschland bestehen vor diesem Hintergrund in zweierlei Hinsicht Strafbarkeitslücken:

1. Ist keine technische Hürde eingebaut, macht sich ein ”Einbrecher“ nicht strafbar, da er nicht ”besonders geschützte“ Daten ausspäht. Freigegebene Windows- Shares sind vom Gesetz ebenso zu behandeln wie freiwillig ins Netz gestellte Webserver. Denn es handelt sich in beiden Fällen um freiwillig ins Netz gestellte, für jedermann ohne technischen Schutz über das Internet abrufbare Inhalte. Ob dies in jedem Fall Absicht ist, darf bezweifelt werden, ist aber für den Nutzer nicht erkennbar.

2. In Deutschland besteht darüber hinaus sogar für das Hacken von Systemen kein strafrechtlicher Schutz, solange Daten nicht ausgespäht oder verändert werden. Der Hacker darf sich also mit Hilfe eines Exploits die Möglichkeit verschaffen, Root- Rechte auf einem System zu erlangen, solange er diese Möglichkeit nicht zum Anschauen oder "Korrigieren" der Daten nutzt. Die Kenntnis dieser Lücken ist wichtig für die eigene Absicherung, da man ohne technische Hürden dem Angreifer die Chance läßt, auch ohne strafbare Handlung an vertrauliche Daten zu kommen. Ohne die Mithilfe der Staatsanwaltschaft hat man z.B. wegen der fehlenden Zuordnung von Telefonnummer und IP-Adresse, in der Regel keinerlei Chancen auf Verfolgung des Täters und Schadensersatz.

Veröffentlichung von Hackertools und Sicherheitslücken notwendig

Gesetzgebungsbedarf gab es dagegen für Deutschland im Bereich der Verbreitung von Passworten und anderen Zugriffsberechtigungen oder -methoden. Zur Umsetzung der EU-Richtlinie vom 20.11.1998 hat der Bundestag am 01.02.2002 den Entwurf eines Zugangskontrolldiensteschutzgesetzes verabschiedet, ohne die Einwände des Bundesrates und meines c't-Artikels (Hackertools im Visier der Justiz, Heft 02/2002, Seite 76) zu berücksichtigen. Danach hat das Gesetz am 22.03.2002 den Bundesrat passiert und ist am darauf folgenden Tag in Kraft getreten.
Das Benutzen von geknackten Schlüsseln oder Passworten zur kostenlosen Nutzung von kostenpflichtigen Fernseh- oder Online-Angeboten war nach § 265a StGB oder § 263a StGB bereits vorher unter Strafe gestellt. Da diese Art von Straftaten zu Hause schon wegen des Schutzes der Privatsphäre nach Art 13 GG kaum entdeckt werden können und ein großer Schaden für die Urheberrechtsinhaber droht, war es notwendig, schon im Vorfeld der eigentlichen Rechtsverletzung einzugreifen. In Zukunft werden schon im Vorfeld des § 265a StGB bereits die Verbreitung von Passwort-Listen, von Knackprogrammen für Pay-TV oder Schlüsselgeneratoren für Shareware- Programme unter Strafe gestellt.

Mit dem deutschen Zugangskontrolldienstegesetz werden gleichzeitig die Forderungen von Artikel 6 der Cybercrime-Konvention sowie diejenigen der entsprechenden EU-Richtlinie vollständig erfüllt.

Das Gesetz kann in der derzeitigen Fassung aber mehr Probleme als Lösungen bringen, da es zu weit gefasst ist und unerwünschte Nebeneffekte auftreten können.

Vom Wortlaut des Gesetzes her ist der Zweck der Verwendung von Entschlüsselungstools nicht spezifiziert. Die Strafbarkeit kann daher neben den Software- und TV-Piraten auch Security Consultants erfassen, die im Auftrag von Kunden Netzwerke auf deren Verwundbarkeit testen.

Der Bundesrat nahm am 27.9.2001 dazu Stellung:

> *Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren in geeigneter Weise klarzustellen, dass Zugangskontrolldiensteanbieter, die Umgehungsvorrichtungen verwenden, um Zugangskontrolldienste auf ihre Tauglichkeit zu testen bzw. deren Sicherheitsstandards zu verbessern, nicht vom Verbot des § 3 Nr. 1 und 2 ZKDSG und den Straf- und Bußgeldvorschriften in den §§ 5 und 6 ZKDSG erfasst werden.*
>
> *Begründung*
>
> *In diesen Fällen besteht für ein Verbot und damit auch für eine Bestrafung kein Anlass. Der Bundesrat weist auf die ähnliche Problematik bei Artikel 6 des Entwurfs eines Übereinkommens des Europarates über Datennetzkriminalität (Draft Convention on Cyber-Crime) und die diesbezüglichen Ausführungen in Nummer 76 des Entwurfs eines Erläuternden Berichts hierzu hin.*

Die Bundesregierung äußerte sich zur Stellungnahme des Bundesrates wie folgt:

> *Die Bundesregierung hat den Vorschlag geprüft. Die Bundesregierung tritt dem Antrag entgegen. Eine Klarstellung ist nicht erforderlich. Zweck des Gesetzes ist es, zugangskontrollierte Dienste gegen unerlaubte Nutzungen zu schützen. Wenn Zugangskontrolldiensteanbieter Umgehungsvorrichtungen verwenden, um Zugangskontrolldienste auf ihre Tauglichkeit zu testen bzw. deren Sicherheitsstandards zu verbessern, liegt schon kein nach § 3 verbotenes Verhalten vor. Abgesehen davon, dass Tests und Verbesserungen des Sicherheitsstandards zu einem großen Teil schon von den Tathandlungen in den §§ 3, 5 und 6 nicht erfasst*

werden, beziehen sich diese in einem solchen Fall nicht auf technische Verfahren oder Verfahren, die dazu bestimmt oder angepasst sind, die „unerlaubte" Nutzung eines zugangskontrollierten Dienstes zu ermöglichen. Auch liegt kein verbotenes Verhalten „zu gewerbsmäßigen Zwecken" vor. Schließlich liegt auch noch eine Einwilligung der von den §§ 3, 5 und 6 geschützten und verfügungsberechtigten Zugangskontrolldiensteanbieter vor.

Diese Gegenäußerung vermag aber aus logischen und juristischen Gründen in keiner Weise zu befriedigen. Erstens kann die Definition „unerlaubt" in einem Straftatbestand kein zusätzliches Kriterium bieten, da dies zu einem Zirkelschluss führen würde: „Wenn es unerlaubt ist, dann ist es nach diesem Gesetz nicht erlaubt!". Zweitens greift die angesprochene Verfügungsberechtigung der Rechteinhaber nicht in jedem Fall, da der Netzwerkbetreiber und der Inhaber des Urheberrechts an der geknackten Software in der Regel auseinanderfallen. Damit ist nicht klar aus dem Gesetz erkennbar, wer mit seiner Einwilligung die Strafbarkeit der Security-Firma verhindern kann.

In diesem Fall können sich die Administratoren nicht mehr ausreichend über den Schutzbedarf informieren und Lücken selbst nicht mehr testen. Netzwerksicherheitsexperten würden sowohl bei ihren Sicherheitstests als auch bei Hackerschulungen für Systemadministratoren durch eine solche Interpretation schwer behindert.

Um die Sicherheit von Netzen effektiv testen zu können, müssen Security-Firmen die gleichen effektiven Hilfsmittel benutzen können wie die Hacker selbst. Daher würden die Security-Experten in dem Hase-und-Igel-Spiel Firewall-Sicherheit noch weiter an Boden verlieren, weil sich die Hacker weiterhin unter Verstoß gegen das Gesetz der Hilfsmittel bedienen werden.

Microsoft kann sich aus einem anderen Grund über das Gesetz freuen: Jede Linux-Distribution enthält bereits in der Standard-Variante zahlreiche Tools, die vom Wortlaut des Gesetzes erfasst werden. Weder den Linux-Distributoren noch den Netzwerk-Security-Firmen wird die Beschränkung auf die Gewerbsmäßigkeit etwas helfen, da diese solchen Firmen wie der Suse Linux AG kaum abzusprechen ist.

Geplante weitere Verschärfungen des Urheberrechtsschutzes

Die Bemühungen der Urheberrechtslobby zu effektiveren Schutzmassnahmen gehen aber weiter und schießen noch weit darüber hinaus. Die neue EU-Urheberrechtsrichtlinie lässt für die Umsetzung in deutsches Recht relativ viel Spielraum, was Erlaubnis oder Verbot privater Kopien anlangt.
Der vorliegende Entwurf verschärft die derzeit geltende Rechtslage. Es wird zwar das bestehende Recht auf die private Kopie beibehalten, aber die Umgehung von Kopierschutzmechanismen soll in Zukunft in jedem Fall verboten werden, auch dann, wenn bisher die Privatkopie trotz Kopierschutz erlaubt war. Bei Privatleuten soll allerdings keine Strafbarkeit daran gebunden werden.

Den Urheberrechtsinhabern geht selbst diese Änderung nicht weit genug. Es wird von diesen angestrebt, zwingend Digital Rights Management Mechanismen einzuführen. In einem Entwurf des „Security System and Copyright Act" in den USA wird in einem noch weitergehenden Schritt sogar gefordert, dass die Industrie nur noch Computer mit vorinstalliertem Digital Rights Management System ausliefern darf.

Die Firma Microsoft könnte damit ihre beherrschende Marktposition noch weiter festigen, da sie Inhaberin mehrerer Patente im Bereich Digital Rights Management ist und die Verbreitung von Linux und anderen Betriebssystemen effektiv torpedieren könnte.

Durch das Zugangskontrolldienstegesetz dürfte die Qualität dieser DRM-Modelle und deren evtl. vorhandene Spionageaktivität durch Übertragung von Lizenzinformationen auf legale Weise nicht mehr untersucht werden. Wenn man sich die Funktionalität des Windows Media Players in der Version 8 einmal genauer anschaut, kann man sich etwa vorstellen, welche Spionage-Möglichkeiten sich zukünftig unter dem Deckmantel des Urheberrechts auftun. Bei Windows XP lässt sich Microsoft schon jetzt im Lizenzvertrag das Recht einräumen, jederzeit auf den Rechner des Nutzers zugreifen zu können. Darüber hinaus ist ein User vorinstalliert, der dies auch technisch ermöglicht.

Fazit

Durch die Beteiligung von Lobbyisten an der Erarbeitung von Gesetzesentwürfen werden häufig berechtigte Interessen wie z.B. diejenigen der IT-Security-Branche nicht genügend berücksichtigt. Dies geschieht leider in letzter Zeit häufiger: Auch bei der Änderung des Teledienstedatenschutzgesetzes durch das Elektronische Geschäftsverkehrsgesetz sind ausnahmsweise Speicherungsrechte auf Fälle des Abrechnungsbetrugs beschränkt worden, während noch im Gesetzentwurf vom 14.02.2001 auch andere Sicherheitsverletzungen berücksichtigt wurden.
Durch die unklare Gesetzesformulierung des Zugangskontrolldienstegesetzes wird es in Zukunft immer wieder zu Irritationen bezüglich der Zulässigkeit z.B. von Hackerschulungen für Systemadministratoren oder von Penetrationstests kommen, obwohl man dies auf Anregung des Bundesrates hätte klar und deutlich formulieren können. Wenn man an die eigenwillige Gesetzesauslegung durch Richter wie im Fall des früheren Compuserve-Chefs Somm denkt, kann man jetzt schon die Gefahren erkennen, in die Security Consultants zukünftig geraten könnten.