IN DEUTSCHLAND GIBT ES IMMER NOCH GESETZESLÜCKEN

Neue Geschütze im Kampf gegen Internet-Piraten und Cyber-Terroristen

Allmählich wird es enger für Hacker und Premiere-Schwarzseher in Deutschland: Mit dem Zugangskontrolldiensteschutzgesetz ist das Anbieten von Crack-Software für analoge oder digitale Zugänge im Internet seit 23. März unter Strafe gestellt. Ulrich Emmert* erläutert, wo auch jetzt noch Gefahr durch Hintertürchen für Hacker droht.

Bisher nutzen Hacker die fehlende internationale Harmonisierung der Strafrechtsvorschriften perfekt aus. In den relativ liberalen Niederlanden konnten zum Beispiel Musiktauschbörsen, Raubkopie- und Pornoanbieter noch bis vor kurzem weitgehend unbehelligt ihrer Tätigkeit nachgehen. Staaten wie Togo vergeben beispielsweise Domains, die nirgendwo einem Besitzer zugeordnet werden können und daher häufig zu illegalen Zwecken missbraucht werden.

Cybercrime-Abkommen des Europarats

Diesen Problemen will man zumindest im europäischen Rahmen zu Leibe rücken. Am 9. November 2001 wurde der 27. Diskussionsentwurf des Cybercrime-Abkommens des Europarats endgültig abgesegnet. Seit 23. November 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 sowie die internationale Zusammenarbeit verbessert werden.

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 Mitgliedstaaten des Europarats, fehlen bislang einzelne oder auch eine ganze Reihe von Strafvorschriften, um die Cyber-Kriminalität wirksam bekämpfen zu können.

Im Bereich Hacking sollen der unerlaubte Zugriff auf Rechnersysteme, das Abhören und Sniffen von Daten, die Störung oder Veränderung der Kommunikation, das Stören 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 Mitgliedstaaten unter Strafe gestellt werden. Beim Ausspähen von Daten wird den Mitgliedstaaten die Möglichkeit gegeben, 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:

- 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.
- 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 Exploit die Möglichkeit verschaffen, Root-Rechte auf einem System zu erlangen, solange er diese Möglichkeit nicht zum Anschauen oder „Korrigieren" der Daten

Fortsetzung auf Seite 30

...rtsetzung von Seite 29

...tzt. Die Kenntnis dieser Lücken ...t wichtig für die eigene Absiche...ng, da man ohne technische Hür...en dem Angreifer die Chance ...sst, auch ohne strafbare Hand...ng an vertrauliche Daten zu kom...en. Ohne die Mithilfe der Staats...waltschaft hat man beispiels...eise wegen der fehlenden Zuord...ung von Telefonnummer und IP-...dresse in der Regel keine Chance ...f Verfolgung des Täters und ...chadensersatz.

...decken von ...icherheitslücken nötig

...esetzgebungsbedarf gab es dage...en für Deutschland im Bereich ...er Verbreitung von Passworten ...nd anderen Zugriffsberechtigun...en oder -methoden. Zur Umset...ung der EU-Richtlinie vom 20. No...ember 1998 hat der Bundestag am ... Februar 2002 den Entwurf eines ...ugangskontrolldienstesschutzgesetz...es verabschiedet, ohne die Ein...wände des Bundesrates zu berück...sichtigen. Dennoch hat das Gesetz ...m 22. März den Bundesrat pas...iert und ist am darauf folgenden ...ag in Kraft getreten.

...isher war die Verbreitung von ...Programmen zum Knacken von ...Shareware durch keinen Straftat...bestand unterbunden. Mit dem ...eutschen Gesetz werden bereits ...etzt vor der Unterzeichnung und ...ntifizierung die Forderungen von ...rtikel 6 der Cybercrime-Konven...tion erfüllt. In Zukunft wird bereits ...ie Verbreitung von Passwort-Lis...ten, von Knackprogrammen für ...ay-TV oder Schlüsselgenerato...ren für Shareware-Programme un...ter Strafe gestellt. Abgrenzungs...chwierigkeiten wird es dabei zwi...schen Passworten und Security ...Exploits geben.

...ürften, wie Microsoft im Gegen...satz zum Gesetzentwurf vorschlug, auch keine Sicherheitslücken und Programme zur Identifikation die...ser Lücken mehr veröffentlicht werden, würde das Netz noch unsi...cherer. In diesem Fall könnten sich die Administratoren nicht mehr ausreichend über den Schutzbe...darf informieren und Lücken selbst nicht mehr testen. Netz...werksicherheitsexperten würden ...sowohl bei ihren Sicherheitstests als auch bei Hackerschulungen für Systemadministratoren durch eine solche Interpretation schwer be...hindert.

Weitere Straftaten, die nach der Cybercrime-Konvention verfolgt werden sollen, sind Kinderporno...grafie, rassistische Äußerungen sowie Urheberrechtsverletzungen.

Datenschutz weiter eingeschränkt

Der zweite Teil der Cybercrime-Konvention befasst sich mit dem Verfahren der Überwachung von Internetdaten durch die zuständigen Behörden und deren Datenaustausch. In Deutschland werden die dort geforderten Maßnahmen größtenteils bereits jetzt aufgrund der Terroranschläge in den USA vom 11. September 2001 umgesetzt. Nach dem zweiten Anti-Terror-Gesetz vom 11. Januar 2002, das in Berlin nach Innenminister Otto Schily nur noch „Otto-Katalog" genannt wird, sollen sämtliche Verbindungsdaten im Internet dem Zugriff von staatlichen Stellen unterliegen.

Damit werden die bisherigen Datenschutzvorschriften auf den Kopf gestellt: Während es bisher verboten war, Nutzerdaten nach Ende der Nutzung außer zu Abrechnungszwecken aufzubewahren, wird jetzt das Loggen erlaubt, in manchen Fällen sogar zur Pflicht. Schon bisher dürfen Verfassungsschutz, Bundesnachrichtendienst, militärischer Abschirmdienst, das Zollkriminalamt und die Strafverfolgungsbehörden Fernmeldeüberwachung durchführen, jeweils auf verschiedener Rechtsgrundlage.

Für die Dienste ist dies im Gesetz zu Artikel 10 Grundgesetz geregelt. Der Verfassungsschutz darf im Inland bei Verdacht von Straftaten im Bereich des Verfassungsschutzes abhören, der Bundesnachrichtendienst im Ausland oder bei Verbindungen ins Ausland in jedem Fall. Die Staatsanwaltschaft kann nur bei einem Katalog schwerer Straftaten von diesem Instrument Gebrauch machen, während das Zollkriminalamt nicht nur bei Zollvergehen, sondern auch bei Verstößen gegen das Kriegswaffenkontrollgesetz im Wege der Fernmeldeüberwachung ermitteln darf.

Das Zweite Anti-Terror-Gesetz schränkt den Datenschutz zu Gunsten der Ermittlungsbehörden deutlich ein. Das neue Paket enthält vor allem ein ganzes Maßnahmenbündel zur Erweiterung von Ermittlungskompetenzen, bleibt aber gegenüber dem ursprünglichen Entwurf nicht zuletzt wegen der deutlichen Kritik von Bürgerrechtlern und Grünen erheblich zurück.

Verfassungsschutz und Bundesnachrichtendienst erhalten Auskunftsrechte gegenüber Banken, Finanzdienstleistern, Sozialversicherungen und Luftfahrtunternehmen. Zusätzlich gibt es erweiterte Möglichkeiten, auf Verbindungsdaten im Internet oder auf Aufenthaltsorte von Mobiltelefonen zuzugreifen.

Die ursprünglich geforderte Speicherungspflicht für Internet-Nutzungsdaten ist aber im Gesetz vom 11. Januar 2002 nicht mehr enthalten. Die tatsächlich vorhandenen Daten sollen auf Anfrage den zuständigen Stellen nach der neuen Telekommunikationsüberwachungsverordnung jederzeit zugänglich gemacht werden müssen. Künftige Datenverbindungen von verdächtigen Personen müssen auf Verlangen der Behörden von Providern mitgeschnitten und übermittelt werden.

Die Überwachung wird von der Regulierungsbehörde vorgenommen, die allerdings kein eigenes Prüfungsrecht hat, ob die angeordnete Überwachung rechtmäßig ist. Die Telekommunikationsüberwachungsverordnung verpflichtet nur Firmen, die Telekommunikationsdienstleistungen für die Öffentlichkeit anbieten. Ursprünglich war geplant, auch interne Kommunikationsleitungen und interne Gespräche von Firmentelefonanlagen abhörbar zu machen.

Die Kosten für die Überwachungsmaßnahmen werden den Providern auferlegt, was bei kleineren Providern zu existentiellen wirtschaftlichen Problemen führen kann. In der Verordnung ist nun daher für kleine Provider eine Ausnahmeregelung geschaffen worden, was wiederum aber die Effektivität der Maßnahme in Frage stellt.

Zweifel an der Effektivität der Überwachung

Die Effektivität von Überwachungsmaßnahmen in Bezug auf den Datenverkehr ist mehr als zweifelhaft. Terroristen, professionelle Wirtschaftskriminelle oder Drogendealer, die als Ziel der Überwachungsmaßnahmen angeführt werden, sind jederzeit in der Lage, sich diesen Maßnahmen vollständig zu entziehen. Durch die Nutzung der starken Verschlüsselung mit Programmen wie beispielsweise Pretty Good Privacy (www.pgpi.org) können Inhalte auch vor Strafverfolgungsbehörden und Geheimdiensten geschützt werden.

Ein Verschlüsselungsverbot, wie es von den Geheimdiensten auch in Deutschland gefordert wird, ist sinnlos, da sich genau diejenigen, die man überwachen will, nicht an das Verbot halten werden. Terroristen, die Flugzeuge entführen oder Menschen ermorden, kann man mit einer Strafandrohung von einem oder zwei Jahren wegen Verstoßes gegen ein Verschlüsselungsverbot keine Angst einjagen.

Die „braven" Bürger und Firmen hingegen würden einen erheblichen Verlust an Vertraulichkeit erleiden, der sie dem Hacking und der Wirtschaftsspionage schutzlos ausliefert. In der Praxis würden die Strafverfolgungsbehörden nicht einmal bemerken, dass verschlüsselte Informationen übertragen werden, da hierzu die Technik der Steganographie verwendet werden kann. Dabei werden verschlüsselte Informationen in Bildern mit hoher Farbanzahl oder Tondateien versteckt, ohne diese erkennbar zu verändern. Ohne die Eingabe des richtigen Passworts kann nicht festgestellt werden, ob überhaupt Daten versteckt wurden. Solche Programme sind als Shareware für jedermann im Internet erhältlich (www.steganos.de).

Daher fängt man durch ein solches Verschlüsselungsverbot kaum technisch versierte Verbrecher, sondern vorwiegend Kleinkriminelle. Es ist sehr zweifelhaft, ob sich dafür der riesige Aufwand der Überwachung lohnt und nicht der Aufwand den Nutzen bei weitem übersteigt. Das Gebot der Verhältnismäßigkeit kann bei diesem erheblichen Eingriff in die Freiheitsrechte des Bürgers kaum eingehalten werden.

Bisher konnten nur die Abrechnungsdaten bei volumenbezogener Abrechnung bis 80 Tage nach Rechnungsversand gespeichert werden. Die Frist von 80 Tagen ist durch die Neufassung des Teledienstedatenschutzgesetzes auf sechs Monate verlängert worden. Durch eine Gesetzesänderung sollte zur Bekämpfung der missbräuchlichen Nutzung auch die Möglichkeit geschaffen werden, [illegible] solche Nutzungsdaten, bei denen ein konkreter Verdacht besteht, zur Rechtsverfolgung zu speichern. Leider wurde diese zur Rechtsverfolgung von Hackerangriffen sinnvolle Regelung auf Abrechnungsbetrug beschränkt und damit der Internetsicherheit ein Bärendienst erwiesen.

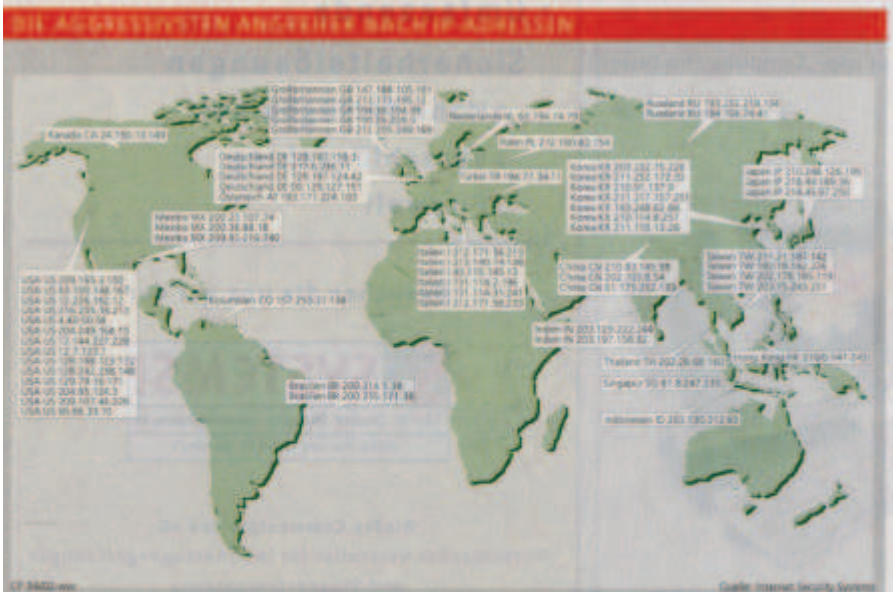
Auf der einen Seite werden den Sicherheitsbehörden weitreichendere Befugnisse zur Cybercrime-Bekämpfung in die Hand gegeben, auf der anderen Seite hindert man aber die Firmen durch den Datenschutz daran, das eigene Netz effektiv gegen Angriffe zu schützen, weil eine nachträgliche Auswertung von Logdateien nur bei Abrechnungsbetrug möglich ist.

Mit der europaweiten Vereinheitlichung des Hackerstrafrechts wird ein wertvoller Beitrag zur Internetsicherheit geleistet. Die Erweiterung der Überwachungsmaßnahmen durch den Staat werden aber gerade bei der erklärten Zielgruppe kaum effektiv sein, da sich diese der Überwachung gezielt entziehen kann. Vor diesem Hintergrund ist es fraglich, ob die damit verbundenen Einschränkungen der Privatsphäre und des Geheimnisbereichs von Firmen erforderlich und verhältnismäßig sind.

Gänzlich unverständlich ist dabei, dass den Firmen selbst nur bei Abrechnungsbetrug und nicht bei anderen Hackerangriffen die weitere Speicherung von Logdateien gestattet werden soll.

www.kanzlei.de/onlinerecht.htm
www.hamburg.ccc.de/cybercrime

**Ulrich Emmert ist Anwalt bei der Kanzlei ESB Rechtsanwälte und arbeitet unter anderem im Auftrag des Fachdistributors Icon Systems.*



Die aggressivsten Hacker sind in den USA und Korea beheimatet. In Europa geht die meiste Gefahr von Italien, Großbritannien und Deutschland aus.