PANAMP.DE 2007

© 2007 PAN AMP AG

[DER HACKERPARAGRAF IST DER GRÖßTE UNSINN]

Hackertools zu nutzen, auch wenn es der eigenen Sicherheit dient, ist künftig verboten. PAN AMP Vorstand Bert Weingarten fordert in einem Gastbeitrag ein Eingreifen des Bundespräsidenten.

Hamburg/Berlin, den 16. Juli 2007

Hackertools zu nutzen, auch wenn es der eigenen Sicherheit dient, ist künftig verboten. PAN AMP Vorstand Bert Weingarten fordert in einem Gastbeitrag ein Eingreifen des Bundespräsidenten:

Mit großer Sorge um die weitere Standortattraktivität Deutschlands muss ich eine beispiellose gesetzliche Fehlentwicklung feststellen, was die IT-Sicherheit und die Abwehr von Industriespionage via Internet angeht.

Per EU-Rahmenbeschluss wurden die Mitgliedstaaten der Europäischen Union bis zum 16. März 2007 verpflichtet, Maßnahmen zur Bekämpfung der Computerkriminalität zu treffen. In Deutschland entstand hierzu u.a. der so genannte Hackerparagraf. Es handelt sich dabei um Paragraf 202 c des Strafgesetzbuches, der mittlerweile den Bundestag und den Bundesrat passiert hat und nun nur noch auf die Unterschrift des Bundespräsidenten wartet.

Einhellige Ablehnung

In meiner bisherigen Berufslaufbahn habe ich es noch nie erlebt, dass ein Gesetzentwurf derart umfassende Ablehnung erfährt. Professoren, Sicherheitsbeauftragte und IT-Hersteller lehnen den Entwurf genau so ab wie die Fachpresse und zahlreiche Computer-Vereine. Mir ist kein einziger IT-Sicherheitsexperte bekannt, der den Gesetzesentwurf unterstützt.

Um Klarheit in die rechtlichen Konsequenzen des Entwurfes zu bringen, hat die PAN AMP AG, deren Vorstand ich bin, Mittel bereitgestellt und Juristen beauftragt. Diese kamen zu dem Ergebnis, dass in dem Gesetzesentwurf eine Vielzahl von Ungereimtheiten verankert sind. Ich finde es beachtlich, dass der Entwurf in dieser Form vorgelegt wurde.

Beispielhaft möchte ich mögliche rechtliche Konsequenzen anhand eines Absatzes des Gesetzentwurfes ausführen. An einer Stelle des Paragrafen 202 c heißt es: «Wer Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft».

Konsequenzen für Unternehmen …

Anders gesagt: Wer Passwörter, sonstige Sicherheitscodes für den Datenzugang oder geeignete Computerprogramme herstellt, beschafft, verkauft, überlässt, verbreitet oder zugänglich macht, beteiligt sich an der Vorbereitung einer Straftat und wird mit Geld- oder Freiheitsstrafe von bis zu einem Jahr bedroht. Das kann weitreichende rechtliche Konsequenzen haben.

Konzerne, der Mittelstand und Innovationsträger könnten zukünftig keine Sicherheitsüberprüfung Ihrer Netzwerke und Ihrer Online-Dienste mehr geliefert bekommen, da IT-Experten solche Aufträge nur unter Verwendung entsprechender Sicherheitssoftware leisten können. Eine ständige Überprüfung auf Sicherheitslücken

wird u.a. mit Hackertools durchgeführt. Sie sind zur Abwehr von Industriespionage und Systemmanipulationen unverzichtbar.

Durch den Gesetzestext aber macht sich der Auftragnehmer, der einen Sicherheitstest erbringen will, strafbar. Dies gilt auch für den Fall, dass der Auftragnehmer dem Auftraggeber Hackertools zur Verfügung stellt. Eine fortlaufende Sicherheitsprüfung darf auch im direkten Auftragsverhältnis nicht mehr erfolgen.

... für die Ausbildung ...

Auch die Ausbildung von Internet-Fahndern würde kriminalisiert. Aktuell arbeite ich einem Projekt zur Ausbildung staatlicher Internet-Fahnder. Etwa ein Fünftel des Studiums behandelt das Erlernen und die Anwendung von Sicherheits-Software und -Tools.

Käme Paragraf 202 c zur Anwendung, so würde nach Einschätzung unserer Anwälte aus mir ein Krimineller – obwohl ich staatliche Internet-Fahnder ausbilde. Betroffen wären auch für Professoren der Informatik an Universitäten und Fachhochschulen, die den Bereich IT-Sicherheit unterrichten.

... und für die Software

Eine Vielzahl von Betriebssystemen beinhaltet seit Jahren Hackertools. So sind z.B. in vielen Linux-Versionen Tools wie Nmap, tcpdump und andere enthalten. Künftig könnten sie unter Verbot stehen. Da es sich bei Linux-Versionen um meist kostenlos erhältliche Betriebssysteme handelt, sind die entsprechenden Installationsdateien millionenfach auf Downloadservern im Internet verbreitet. Es müssten also alle Linux-Versionen auf deutschen Server gelöscht werden, die auch nur ein Tool des „Hackerparagrafen“ enthalten. Jeder Anbieter dieser Versionen - Universitäten, Archive und die Industrie - macht sich ansonsten strafbar.

Bert Weingarten

Foto: PAN AMP AG

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt ein freies Tool zur Überprüfung der Sicherheit von Systemen im Netzwerk zur Verfügung. Die so genannte BSI Open Source Security Suite (BOSS) beruht u.a. auf dem Schwachstellenscanner Nessus. Um die Benutzerfreundlichkeit von Nessus zu steigern, wurde eine grafische Oberfläche hinzugefügt. Nessus ist als Hackertool anwendbar. Nach dem Inkrafttreten des Paragrafen 202 c würde die BSI-Software illegal.

Unklare Nachbesserungen

Der Gesetzentwurf ist in der aktuellen Variante der größte Unsinn, der mir in meiner bisherigen Berufslaufbahn untergekommen ist. Es ist völlig unverständlich, warum das Bundesamt für Sicherheit in der Informationstechnik gegen diesen Unsinn nicht massiv interveniert hat.

Ende Mai 2007 hat der Bundestag mit den Stimmen von CDU/CSU, SPD, FDP und den Grünen das Gesetzesvorhaben in letzter Lesung verabschiedet. In einem persönlichen Gespräch mit dem stellvertretenden Vorsitzenden der CDU/CSU-Bundestagsfraktion Dr. Wolfgang Bosbach gelang es mir, seine Aufmerksamkeit auf eine Überarbeitung des Paragrafen 202 c vor dem Inkrafttreten zu lenken. Ein gemeinsamer Termin mit dem Innen- und Rechts-Ausschuss der CDU/CSU-Bundestagsfraktion konnte vor der Sommerpause jedoch nicht mehr erfolgen.

Der Rechtsausschuss des Deutschen Bundestages hat zwischenzeitlich eine Zusatzerklärung verabschiedet. Sie soll dafür sorgen, dass von der neuen Regelung nur Computerprogramme betroffen sind, mit denen Straftaten begangen werden können. Allerdings ist unklar, inwieweit diese Erklärung vor Gericht Berücksichtigung finden wird.

In der IT-Rechtssprechung sind schon bisher Urteile deutscher Gerichte nur selten einheitlich und auch nicht immer von IT-Experten nachvollziehbar.

Der Paragraf 202 c eignet sich somit bestens, eine neue Dimension der Nichtnachvollziehbarkeit von Gerichtsurteilen herzustellen. Da der Gesetzentwurf noch nicht einmal eine eindeutige Definition dessen liefert, was überhaupt ein Hackerprogramm ist, müssen demnächst wohl die Richter die Hausaufgaben der Politik machen. Und das, obwohl kaum ein Richter in Deutschland IT-Expertenwissen aufweisen kann.

Eine glatte Sechs

Kurz: Die Novelle des Strafgesetzbuches, bei der u.a. der Paragraf 202 c eingeführt wurde, führt zu extrem negativen Auswirkungen in der Informations- und Innovationssicherheit. Sie belastet somit die Standortattraktivität Deutschlands. Hält ein Richter sich zukünftig an die Novelle, so werden aus verantwortungsvollen Leistungsträgern unserer Gesellschaft Kriminelle. Das Gesetz ist inhaltlich eine glatte Sechs.

Das bereits überarbeite Gesetz bedarf dringend einer grundlegenden Überholung und zwar vor der Verkündung im Bundesgesetzblatt. Ohne eine solche Überarbeitung wird die IT-Sicherheit in Deutschland einen bislang nicht da gewesenen Einschnitt erleiden, da es Experten per Gesetz untersagt wird unverzichtbare Sicherheitsleistungen zu erbringen.

Einzig die Weigerung des Bundespräsidenten, seine Unterschrift zur Ausfertigung zu leisten, könnte das Inkrafttreten des Gesetzes verhindern.

Zur Prüfung der vorgetragenen Punkte habe ich unsere Unterlagen und Ausarbeitungen dem Bundespräsidenten Dr. Horst Köhler zugestellt und um Prüfung gebeten. Ich vertraue auf unseren Bundespräsidenten!

Bert Weingarten

Vorstand, PAN AMP AG

Erstveröffentlichung erfolgte am 16. Juli 2007 als Gastbeitrag in der Netzeitung (http://www.netzeitung.de).

Mehr im Internet:

http://panamp.de

http://www.bundespräsident.de

http://www.bsi.de

Bert Weingarten ist Vorstand des auf IT-Sicherheit spezialisierten Hamburger Unternehmens PAN AMP AG. Als Berater des Vorsitzenden des Bundes Deutscher Kriminalbeamter trägt er Innenministern, Polizeipräsidenten und Politikern Verbesserungsvorschläge zur Inneren Sicherheit vor.

Stichwort: Hackerparagraf

Paragraf 202 c, von Kritikern meist "Hackerparagraf" genannt, heißt offiziell "Strafrechtsänderungsgesetz zur Bekämpfung von Computerkriminalität". Ende Mai wurde er im Bundestag mit großer Mehrheit verabschiedet. Im Juli stimmte auch der Bundesrat zu. Damit der Paragraf in Kraft treten kann, muss ihn der Bundespräsident noch unterschreiben und eine Veröffentlichung im "Bundes-gesetzblatt" erfolgen.

Das Gesetz stellt unter anderem den Besitz, die Verwendung und die Verbreitung von so genannten Hackertools unter bestimmten Umständen unter Strafe. Diese Umstände sind im Gesetzestext sehr vage formuliert. In einem Brief hat unser Gastautor Bert Weingarten den Bundespräsidenten aufgefordert, das Gesetz nicht passieren zu lassen.