2007/30 Lifestyle

https://www.jungle.world/artikel/2007/30/waffenschein-fuer-linux

Waffenschein für Linux!

Von **Burkhard Schröder**

Wer kennt noch einen Dietrich? Das kleine Gerät ist ein Hackertool: Es öffnet Türen auf schöpferische Art und Weise und anders als mit einem gewöhnlichen Schlüssel. Hackertools stehen bald unter Strafe. Sobald der neue Paragraf 202c des Strafgesetzbuchs in Kraft tritt, stehen viele Systemverwalter und Netzwerktechniker mit einem Bein im Gefängnis und sind mit Berufsverbot bedroht. Software, die überprüft, ob ein System oder ein einzelner Computer Schwachstellen hat, eignet sich auch dazu, in fremde Rechner einzudringen. Wer mit diesen Instrumenten arbeitet, wird vom Hackertool-Paragrafen zum potenziellen Verbrecher erklärt. von burkhard schröder

Trotz vehementer und einhelliger Kritik fast aller IT-Experten, Lobbygruppen und der Branchenverbände hat sich die Bundesregierung nicht davon abhalten lassen, das neue Gesetz zu beschließen. Es drängt sich der Verdacht auf, wie schon beim Thema Online-Durchsuchung, dass die Verantwortlichen keinen blassen Schimmer haben, wovon sie reden und was sie da beschlossen haben. »Besserer Schutz vor Hackern, Datenklau und Computersabotage«, wie es das Ministerium formuliert? Mitnichten, bestenfalls ein gut gemeintes und populistisches Placebo nach dem Motto: Bundesregierung verbietet Dietriche und Schraubenzieher – besserer Schutz vor Einbrechern, Juwelenklau und Vandalismus.

Bereits vor sechs Jahren, im November 2001, sollte das Übereinkommen des Europarats Mindeststandards für die Strafvorschriften bei bestimmten Formen der Computerkriminalität herstellen. Das ist an sich sinnvoll, da nationale Gesetze im Internet wenig helfen. Der damals nur von wenigen Fachleuten diskutierte Beschluss des Europarats ist jetzt fast wörtlich übernommen werden. Der § 202c StGB – »Vorbereiten des Ausspähens und Abfangens von Daten« – lautet: »(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er 1. Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder 2. 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.«

Das ist so vage formuliert, dass alle gängigen Programme damit gemeint sein könnten, mit denen Firmen und Netzwerk-Techniker in Deutschland die Sicherheit ihrer Computer überprüfen. Die so genannten Denial-of-Service-Attacken, mit denen Rechner mit sinnlosen Anfragen so überschüttet werden, dass sie blockiert sind oder den Geist aufgeben, dienen unstrittig nicht der Sicherheit, sondern nutzen aus, dass Daten im Internet immer in zwei Richtungen fließen können – eben »interaktiv«. Auch Phishing ist eindeutig kriminell – dem Nutzer wird eine seriöse Website vorgegaukelt, die ihn in Wahrheit seiner privaten Daten, vor allem der Zugangsdaten seiner Konten, beraubt. Phishing ist ein Sonderfall der Computerkriminalität, weil es davon ausgeht, dass jemand unverschlüsselten E-Mails traut und technisch sehr unbedarft ist.

Nessus (**www.nessus.org**) aber ist zum Beispiel ein Programm, das bei vielen Linux-Versionen ohnehin »ab Werk« mitgeliefert wird. Es arbeitet nach dem Prinzip der Fernwartung (remote access) und überprüft Sicherheitslücken des Zielsystems, in dem es an alle möglichen digitalen Türen (ports) »klopft«. Passwortscanner, Portscanner, Netzwerksniffer – alle Tools, die im weiteren Sinn die Fernwartung von Rechnern ermöglichen, können im Sinne des neuen Gesetzes auch als Hackertools benutzt werden.

Die Befürworter des neuen Gesetzes argumentieren, nicht der Datenklau an sich sei strafbewehrt. Es gehe nur um Daten, die als schutzwürdig deklariert wurden. Zum Täter wird man erst dann, wenn man eine wie auch immer geartetete »Zugangssicherung« überwunden habe. Prof. Dr. Eric Hilgendorf von der Universität Würzburg, einer der zum neuen Gesetzesentwurf angehörten Experten, meint, es sei sogar möglich, dass der strafrechtliche Schutz entfalle, wenn das Opfer nachlässig und fahrlässig mit den eigenen Daten umgegangen sei. Aber auch Jugendliche, die sich das Passwort für Fernsehprogramme im Pay-TV besorgten, die ihre Eltern ihnen verboten haben, machten sich künftig strafbar.

Deutschland hat ohnehin mit die schärfsten Gesetze aller europäischen Staaten gegen Computerkriminalität. Wer sich fremde Daten unbefugt verschafft, ist derzeit schon kriminell. Die Absicht und die Zielgruppe der neuen Version des Gesetzes sind aber deutlicher formuliert. Auf der Website des Bundesjustizministeriums heißt es: »Künftig soll bereits der unbefugte Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen unter Strafe gestellt werden (§ 202a StGB). Ein Verschaffen von Daten wird nicht mehr erforderlich sein. Damit wird klargestellt, dass Hacking strafbar ist.« Nicht nur kriminelle Handlungen werden bestraft, sondern auch der Besitz digitaler Werkzeuge, mit denen man handeln könnte.

Das Bundesjustizministerium und die Sympathisanten des neuen Paragrafen führen an, es spräche nichts gegen Hackertools, wenn diese in guter Absicht benutzt würden, »zum Zwecke der Sicherheitsprüfung oder zur Entwicklung von Sicherheitssoftware«. Entscheidend sei, dass es sich um eine »Tathandlung zur Vorbereitung einer Computerstraftat« handele. Man darf also einen Dietrich benutzen, um die eigene Wohnungstür zu öffnen, wenn man sich ausgeschlossen hat, nicht aber, wenn es eine fremde Wohnung ist? Im Gesetz steht es anders und unscharf: Alle kostenlosen und quelloffenen Sicherheitsprogramme können zu allen Zwecken benutzt werden. Entweder unterstellt man allen, die an ihnen mitgewirkt haben, finstere Absichten oder dass sie den

Missbrauch billigend in Kauf genommen haben, oder man will nur die Nutzer bestrafen, die Böses damit anstellen. Das ist aber absurd, da man so die Programme nicht aus der Welt schafft und man sich das Gesetz gleich hätte sparen können. Konsequent wäre nur eines, zum Beispiel ein Waffenschein für Linux.

Schon die Experten des Europarats befanden sich in einer Zwickmühle. Einerseits wollten sie offenbar alles verbieten, was die Sicherheit des Datenverkehrs gefährden könnte. Andererseits haben sie seit 2001 den Sicherheitsbehörden immer weitere Befugnisse gegeben, die Bürgerinnen und Bürger zu belauschen und zu überwachen, in deren Privatsphäre einzudringen und Daten zu sammeln. Das Verbot, bestimmte Software in einer bestimmten Absicht zu benutzen, passt zu diesem Trend – jeder Bürger steht unter Verdacht und wird zum potenziellen Verbrecher. Die Behörden und Strafverfolger können im Kampf gegen die Internetkriminalität jedoch nichts anderes tun als alle anderen auch. Wer glaubt, es gebe einen »Bundestrojaner«, muss einräumen, dass man genau den auch gegen den Staat und seine Institutionen einsetzen kann. Wer irrig glaubt, der Staat könne sich in private Rechner hacken und dort Daten jagen und sammeln, sollte sich vor Augen halten, dass das auch andersherum funktioniert.

Bei den aktuellen Gesetzen gegen Hackertools und zur Online-Durchsuchung prallen die Mentalität des klassischen Obrigkeitsstaats und die technische Realität des Internet und des 21. Jahrhunderts aufeinander. Die Idee, man könne Hackertools verbieten, fußt auf der Vorstellung des Informationsmonopols der Herrschenden. Wie bereits in der DDR sollen bestimmte Dinge, die die Untertanen sittlich gefährden oder die diese gegen die Obrigkeit benutzen könnten, in den Giftschrank, ummauert mit Erlaubnissen, Genehmigungen und Durchführungsbestimmungen. Heute jedoch lässt sich ein derartiger Giftschrank nicht mehr verschließen – dem Internet sei Dank.

Das größte Problem ist nicht ein sinnloses Gesetz wie das Verbot, Hackertools zu benutzen, sondern der öffentliche Diskurs, der genauso wenig rational ist wie das Gesetzesvorhaben selbst. Diese Art von Abschreckung funktioniert. Es bleibt bei der Mehrheit das lähmende Gefühl der Ohnmacht gegenüber dem scheinbar allmächtigen und allwissenden Staat und die Furcht, jederzeit strafrechtlich belangt werden zu können, weil die Gesetze so vage formuliert sind, dass sie gegen und für alles ausgelegt werden können.

Ulf Buermeyer, Straf- und Ermittlungsrichter am Berliner Amtsgericht Tiergarten und ehemaliger Netzwerk-Administrator der Universität Leipzig, hat in der Online-Zeitschrift zum Strafrecht (hrr-strafrecht.de) im April einen detaillierten und mit Quellen gespickten Aufsatz verfasst: »Die ›Online-Durchsuchung‹. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme«. Sein Fazit ist einfach: Es habe bisher noch keine einzige erfolgreiche Online-Durchsuchung gegeben, und es werde auch keine geben. Mitte der neunziger Jahre habe es einen Zugriff auf eine Mailbox (Bulletin Board System) und einen offenbar dilettantischen und aus technischen Gründen gescheiterten Versuch gegeben, einem Verdächtigen eine Software ohne dessen Wissen unterzujubeln, um ihn behördlich auszuspionieren. Alles andere sei frei erfunden, auch wenn sogar die »Tagesschau« etwas anderes behauptet habe. Alle Wege der Infiltration fremder Rechner – Ausnutzung von Sicherheitslücken, eine noch zu konstruierende »Bundes-backdoor«,

Manipulation der Internet-Infrastruktur, social engineering – seien schon »mit wenig technischem Sachverstand relativ problemlos zu verstellen«.

Das ändert nichts daran, dass sich die Online-Durchsuchung im kollektiven Unterbewussten festgesetzt hat, weil man den Hackern so gut wie alles zutraut, auch die magische Fähigkeit, überall einzudringen, weil sich die Gegner des Überwachungsstaats an der gruselig schönen Idee berauschen, dass sie schon überall lauern und uns, die Guten, schon umzingelt haben, weil sich bei den Schäubles der Wahn, unter dem digitalen Bett der Untertanen schnüffeln zu können und zu müssen, zu einer fixen Idee verfestigt hat.

Anders formuliert: Die Online-Durchsuchung ist eine mehr oder weniger fromme Legende, eine Wunschvorstellung des Überwachungsstaates, die sich nicht realisieren lässt und höchstens ein paar dumme Kleinkriminelle träfe, als schösse man mit einer Schrotflinte auf eine Gruppe Eichhörnchen mit der Absicht, einen Fuchs zu treffen, der sich vielleicht hinter ihnen versteckt haben könnte. Beim Gesetz gegen Hackertools ist es ähnlich, nur dass der Schütze anschließend das Gewehr noch gegen sich selbst richtet.

© Jungle World Verlags GmbH