Übereifer

Dirk Fox

Je mehr Verbote, desto ärmer das Volk.
Laotse, Dao-de-dsching

Regulierungseifer

Der Regulierungseifer der schon nicht mehr ganz so neuen Bundesregierung hat nun auch die IT-Sicherheit erfasst. Vom Justizministerium wurde der rekordverdächtige Berg von inzwischen 321 eingebrachten Gesetzesvorhaben – fast 30% mehr als der Durchschnitt der bisherigen Rekordlegislaturperiode von 1994-1998 – am 19. September 2006 um einen weiteren Entwurf bereichert. Er enthält eine Überarbeitung des § 202 Strafgesetzbuch, der zahlreiche, bisher nicht erfasste Formen der Computerkriminalität unter Strafe stellt.¹

Tatsächlich wird der unberechtigte Zugriff auf Daten bisher privilegiert behandelt. Denn nur das unberechtigte Sichverschaffen von Daten, „die gegen unberechtigten Zugang besonders gesichert sind“, gilt als Straftat – ein viel zu eingeschränktes Verständnis, das zahlreiche Angriffsarten wie DoS-Attacken oder Trojanische Pferde nicht umfasst. Mit dem am 01. Juli 2004 in Kraft getretenen Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 ist Deutschland nun verpflichtet, Mindeststandards bei der Strafbarkeit bestimmter schwerer Formen der Computerkriminalität umzusetzen.

Wie zuletzt beim umstrittenen Allgemeinen Gleichbehandlungsgesetz (AGG) geht der Entwurf des Justizministeriums jedoch deutlich über das Übereinkommen und den Rahmenbeschluss des EU-Rates über Angriffe auf Informationssysteme vom 24. Februar 2005 hinaus. Denn als „Vorbereitungshandlungen für Computerstraftaten“ sollen nach dem Willen der Justizministerin auch die Herstellung, Überlassung und Verbreitung von Computerprogrammen gelten, „deren Zweck die Begehung einer solchen Tat ist“ (§ 202c StGB neu).

Unverständnis

Nun besitzen Verbote einen unbestreitbaren Vorteil: Mit ihnen wird zielgerichtetes Handeln des Gesetzgebers demonstriert – und diese Klarheit kommt an beim Publikum. Leider besitzt die Wirklichkeit dagegen einen hässlichen Nachteil: Sie ist komplex – und das häufig in größerem Maße, als es der Mensch mit seiner zur Vereinfachung neigenden Wahrnehmung zu erfassen vermag. Das dürfte die tiefere Ursache dafür sein, dass klare Verbote einerseits so beliebt sind – und mit ihnen andererseits oft nicht nur nicht das angestrebte Ziel, sondern sogar dessen Gegenteil erreicht wird.

Beispielhaft lässt sich dies bei der geplanten Änderung des Strafgesetzbuches beobachten, gegen den der Chaos Computer Club, Verbände wie eco und Bitkom sowie Anfang November auch der Bundesrat protestierten – mit ihrer Kritik jedoch auf Unverständnis im BMJ stoßen. Dabei ignoriert die geplante Strafbarkeit von Vorbereitungshandlungen im neuen § 202c wenigstens drei elementare Zusammenhänge:

1. Die öffentliche Verbreitung von Angriffs-Tools ist ein Sicherheitsgarant.

Hacker arbeiten heute überwiegend mit Angreifer-Tools, die im Internet kursieren. Diese sind extrem leistungsfähig, meist Resultat kollektiver Programmierleistung, und erleichtern Hackern das Handwerk erheblich. Zugleich liefern sie ein umfassendes Bild dessen, was Hacker heute können. Aber nur, wenn Hacker-Tools auch weiterhin nicht im Verborgenen wirken, werden wir auch zukünftig wissen, was technisch möglich ist. Das aber ist eine wesentliche Vorbedingung für das Ergreifen angemessener Sicherheitsmaßnahmen. Denn Schutzvorkehrungen kosten Geld – fehlt der Nachweis der Erforderlichkeit, fallen sie dem Rotstift zum Opfer.

2. Die Nutzung von Hacker-Tools steigert die Sicherheit von IT-Infrastrukturen.

Durch den kontrollierten Einsatz von Hacker-Tools lassen sich einerseits Schwach-

stellen der eigenen Infrastruktur aufspüren und andererseits die Sensibilität von Mitarbeitern und Management für die Sicherheit von Informationstechnik sehr wirksam steigern: Wer einmal ein leistungsfähiges Trojanisches Pferd „bei der Arbeit“ erlebt hat, wird das so schnell nicht vergessen.

Das sieht auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) so und verbreitet den Schwachstellen-Scanner Nessus, ein Open-Source-Produkt, seit dem 17. Juni 2005 über ihre BOSS-CD.

3. Ein Hacker-Tool ist von einem Sicherheits-Tool meist nicht unterscheidbar.

Der ehemalige Trojaner Netbus wird heute als Tool für die Remote-Wartung vertrieben. Das Programm Cain & Abel, das einen extrem leistungsfähigen Passwort-Cracker enthält, wird für die Wiedergewinnung vergessener Passwörter empfohlen. So genannte „Penetrations-Testing“ Tools werden regelmäßig von Administratoren zur Überprüfung ihrer eigenen Systeme und Firewalls eingesetzt – in den Händen eines Angreifers liefern sie wertvolle Informationen über Schwachstellen der Infrastruktur. Und die im Kontext der von der Firma RSA ausgerufenen RSA-, RC5- und DES-Challenge entstandenen Crack-Programme lieferten erstmals belastbare Messwerte für den zum Brechen dieser Verfahren erforderlichen Zeitaufwand. Eine „objektive Zweckbestimmung“ solcher Tools ist da schwer auszumachen.

Bemüht man die Analogie zu herkömmlichen (physischen) Schutzmechanismen, fällt zudem ein wesentlicher Unterschied zwischen einem Brecheisen und einem Hacking-Tool ins Auge: Einer Tür sieht man auch so an, ob sie einbruchshemmend verschlossen (oder verschließbar) ist – dem Server, Privatrechner oder der Firewall jedoch nicht. Ohne Penetrationstest muss man blind an die Fehlerfreiheit der inzwischen meist komplexen Konfiguration des Systems glauben.

Vielleicht gibt es bald einen zweiten Unterschied: Die Herstellung und Verbreitung von Brecheisen ist nicht verboten.

¹ Zum Entwurf im Detail siehe Alexander Schultz, in diesem Heft.