SZonNet-Home

leer

Inhaltsverzeichnis

Wissenschaft

Archiv

03.03.98
Die Computerseite

Rätselraten um Code-Knacker

„Einigkeit macht stark“

Anonyme Organisation bricht DES-II-Verschlüsselung

Unbekannte haben einen Wettbewerb (www.distributed.net, SZ vom 5.1.1998) gewonnen, in dem es galt, eine mit dem DES-Verschlüsselungsverfahren codierte Nachricht möglichst schnell zu knacken. Eine weltweit vernetzte Rechnerarmade versuchte sich in den vergangenen an der Aufgabe. Mit dem Preisgeld von 5000 Dollar wollte die Firma RSA Data Security beweisen, daß das DES-Verfahren, mit dem auch Banken zum Teil ihre Transaktionen schützen, nicht sicher ist.

Das Preisgeld soll nun größtenteils an die Free Software Foundation in Boston, USA gehen. Die Organisation sorgt für die Verbreitung kostenloser Qualitätssoftwarekümmert. Der richtige Schlüssel lag im letzten Zehntel aller möglichen Kombinationen, und um ihn zu finden mußten mehr als 90 Prozent aller möglichkeiten durchsucht werden. Daher wurde der codierte Satz erst nach 39 Tagen entdeckt: „Einigkeit macht stark“.

Aufsehen erregte, daß neun Tage nach Beginn des Wettbewerbs sich plötzlich eine anonyme Organisation aus dem Nichts in das weltweite Netz einklinkte und mit mehr als zehn Prozent der gesamten Rechenleistung schlagartig den ersten Platz unter den Teams eroberte. Einzig ihren Namen, www.bitbucket.org, und die freche Herausforderung, der Rest der Welt sollte sich auf seinen Vorsprung von neun Tagen nicht allzuviel einbilden, gab die Gruppe bekannt.

Seitdem reißen die Spekulationen über die Identität dieses Teams nicht ab, zumal es über eine ungeheure Rechenleistung – vergleichbar mit 3000 Pentium Pro-200-Prozessoren – verfügen muß. Denkbar wäre, daß die Verwalter eines großen Firmennetzwerkes dieses zum Knacken des DES-Schlüssels verwendeten. Da solche Netze oft zentral betrieben werden, könnte eine kleine Gruppe entschlossener

Techniker das Entschlüsselungsprogramm auf jedem Rechner der Firma, weltweit verteilt und getarnt, zum Laufen gebracht haben.

Ratlosigkeit bei den Wettbewerbern

Auch ist möglich, daß die anonyme Gruppe einen speziellen DES-Chip entwickelt und dessen Leistung im Wettbewerb getestet hat. Daß ausgerechnet eine anonyme Organisation die sonst so kooperativen Teams von Distributed.Net dominieren würde, hinterließ bei Organisatoren und Teilnehmern des Wettbewerbs eine gewisse Ratlosigkeit. hkl