

COMPUTER

Heimlich auf Sendung

Ein Software-Trick könnte Geheimdiensten helfen, Computer mit einem elektronischen Lauschangriff zu knacken.

Gheimdienste sind wie Schweizer Käse, sagt eine alte Weisheit aus dem Schlapphut-Milieu. Beide haben Löcher, doch durchgucken kann man trotzdem nicht.

Welche Fähigkeiten haben die Späher wirklich? Zum Beispiel darf als gesichert gelten, daß Computer ein beliebtes Spähziel der Geheimen sind. Aber wie lassen sich unbemerkt Bits entwenden? Zwei Forscher sind einer trickreichen Methode auf die Spur gekommen, mit der sich Datentresore knacken lassen.

Sie machen sich zunutze, daß Computer nebenbei kleine Sender sind, denn Rechner verarbeiten Informationen als Spannungsimpulse, von denen mehrere Millionen je Sekunde durch die Schaltungen rasen. Dabei werden elektromagnetische Wellen hoher Frequenz abgestrahlt.

Daß diese Strahlung, außer den Rundfunkempfang zu stören, noch einige andere interessante Effekte hat, demonstrierte ein niederländischer Ingenieur der zivilen Öffentlichkeit schon im Jahre 1985. Wim van Eck war eher zufällig darauf gestoßen, daß man das Bild, das ein PC-Benutzer auf seinem Monitor sieht, mit einem umgebauten Fernseher auch in größerem Abstand empfangen kann. Verantwortlich ist die Bildschirmelektronik. Sie erzeugt kräftige Hochspannungsimpulse, um den Monitor Bildpunkt für Bildpunkt mit Inhalt zu füllen.

Unter dem harmlosen Rubrum „Sonder-elektronik“ bieten diverse Firmen ihrer exklusiven, meist regierungsnahen Klientel spezielle Empfänger an, die diese verräterische Abstrahlung auch über Entfernungen von etwa 100 Metern wieder in lesbare Bilder verwandeln (siehe SPIEGEL 36/1996). Militärs kennen die Methoden schon lange. Sie verlangen für sensible Aufgaben den Einsatz von speziell abgeschirmten „Tempest“-Rechnern, die zum Stückpreis von mehreren zehntausend Mark hermetisch gegen vagabundierende Strahlung abgedichtet sind*.

Was läßt sich alles aus den verräterischen Wellen herauslesen? Der Deutsche

Markus Kuhn, 27, der gerade an der Universität Cambridge an seiner Doktorarbeit schreibt, und der britische Gelehrte Ross Anderson bereicherten die Debatte nun um eine verblüffende Erkenntnis: Durch ein pfiffiges Programm läßt sich ein Computer dazu bringen, unbemerkt intime Daten zu versenden, ohne daß selbst ihr Besitzer sie auf dem Bildschirm sieht.

Kuhns Gerätearsenal ist bescheiden: ein Meßempfänger aus den achtziger Jahren und eine handelsübliche Radioantenne. „Man braucht nur wenig Phantasie, um sich auszumalen, was Profis mit aktuellem

merkliche Variation in das Untergrundgrau eingewoben ist.

In den grafischen Elementen moderner Programmoberflächen – wie Knöpfe, Menüleisten und Bildränder – könnte ein gewitzter Programmierer nach diesem Prinzip Unmengen strahlender Botschaften unterbringen und so zum Beispiel über Stunden oder Tage den Inhalt ganzer Festplatten versenden.

Die Spitzel-Software auf den angegriffenen PC zu schmuggeln ist verhältnismäßig leicht. Diese Aufgabe könnte ein Computervirus übernehmen, das mit einem unverdächtigen Programm, etwa einem Spiel oder einem Bildschirmschoner, in die gegnerische Bastion gelangt.

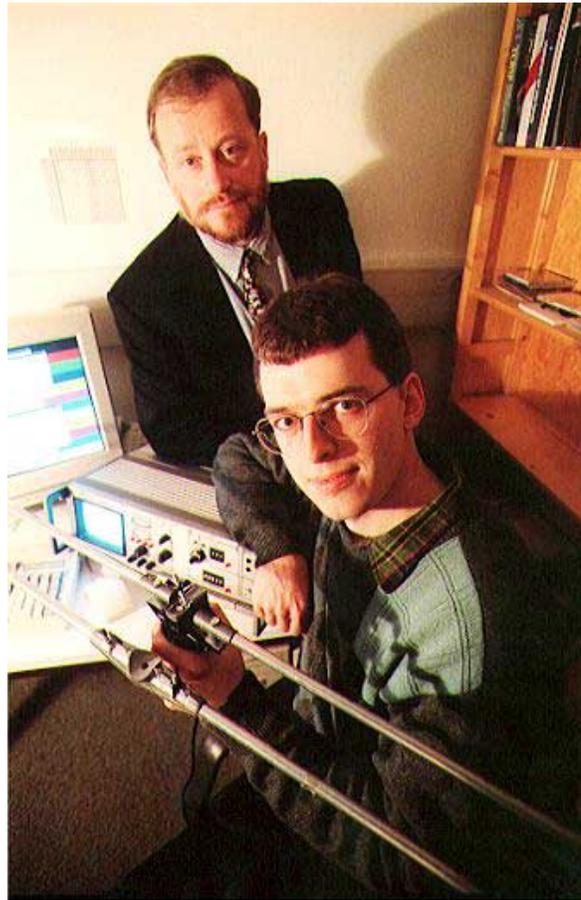
Schon lange spekuliert die Fachwelt, daß Geheimdienste Spähprogramme einsetzen, die sie etwa durch Tarnfirmen ihren Zielobjekten unterjubeln. Doch wie übermitteln die elektronischen Agenten ihre Datenbeute zurück an den Auftraggeber? Bisher schien der Datenklau ausgeschlossen, solange der gefährdete Rechner keinen Kontakt zu Datennetzen hat. Doch offenbar geht es drahtlos genau so.

Ein weiteres Indiz dafür, daß interessierte Kreise bereits intensiv Computer belauschen: Die „Tempest“-Technologie ist so geheim, daß bis heute nicht einmal verraten wurde, nach welchen Kriterien Computer als sicher gelten. Selbst wenn Abschirmungen das sichtbare Monitorabbild in der Abstrahlung unterdrücken, gäbe es diverse Methoden, um softwaregesteuerte Signale à la Kuhn aus dem Rauschnebel herauszufiltern.

Die Forscher reichten ihre Entdeckung zum Patent ein:

„Nur halb ernst gemeint“ (Kuhn) schlugen sie vor, das Senden geheimer Codes lasse sich auch verwenden, um Software-Piraten zu überführen. Die Programme müßten nur unbemerkt ihre Seriennummer vom Bildschirm in den Äther schicken. Peiltrupps könnten dann die Benutzer geklauter Software per Funk orten.

Nach einem Artikel der „Washington Post“ brach im Internet ein Sturm der Entrüstung los. Benutzt der ungeliebte Riese Microsoft sein just in Cambridge gegründetes Forschungslabor, kleine Software-Diebe zur Strecke zu bringen? Doch der Konzern hat die Idee aus der Universität längst verworfen. Das Big-Brother-Image wollte sich die Gates-Firma nicht auch noch aufladen. ♦



Informatiker Kuhn (mit Radioantenne), Anderson
Wie übermitteln elektronische Agenten ihre Beute?

Equipment anstellen könnten“, kommentiert der Jungforscher. Er richtet die Antenne auf einen Monitor, auf dem farbige Testbalken und der Schriftzug „Oxford“ zu sehen sind.

Auf dem kleinen Schwarzweißbildschirm des Testempfängers zeichnen sich prompt die Testmuster ab, doch anstelle des Namens der rivalisierenden Elite-Uni steht hier „Cambridge“.

Kuhn fand heraus, daß bestimmte Helligkeitsmuster auf dem Bildschirm besonders gut abstrahlen, für das menschliche Auge jedoch fast unsichtbar sind. Nur mit der Lupe läßt sich in dem Experiment erkennen, daß das Wort „Oxford“ nicht auf glattem Hintergrund steht, sondern das eingeschmuggelte „Cambridge“ als un-

* Tempest: Abkürzung für „Transient Electromagnetic Pulse Emanation Standard“ (Grenzwerte für kurzzeitig abgestrahlte elektromagnetische Impulse).