Saboteure und Spione im Visier

Tübinger Informatiker arbeiten an intelligentem Abwehrsystem gegen Angriffe im Internet

Im Keller des Wilhelm-Schickard-Instituts auf der Morgenstelle werden akribisch Fingerabdrücke archiviert. Der Chefermittler arbeitet eng mit Spezialisten in der ganzen Welt zusammen. Dieser Kommissar ist kein Kriminologe, sondern Informatik-Professor. Tatort ist das *World Wide Web*, ein Informationsdienst im Internet, auch einfach »das Netz« genannt. Die Rasterfahndung gilt Angriffen von Hackern: Viele treiben Sabotage, als sei das eine neue Sportart. Andere verschaffen sich Zugang zu Bankkonten oder spionieren in geheimen Akten. Deshalb haben Professor Georg Carle und seine Partner bei der Industrie zur Sicherung des Internets ein Forschungsprojekt ins Leben gerufen: Das hochkarätige Glanzstück der Gruppe heißt »Diadem Firewall« und wird von der Europäischen Union gefördert.

Bei manchen Rechnern stehen Hackern Tür und Tor offen. Die in Tübingen entwickelte Diadem-Firewall soll bald alle Sicherheitslücken schließen.

Foto: Bühler

»In jüngster Zeit entwickeln sich regelrechte Bedrohungsszenarien«, stellt Carle die momentane Lage dar. Allein von Juli bis September 2003 sind weltweit 823 neue ›Schädlinge‹ aufgetaucht. Das sind fast 30 Prozent mehr solcher ›Viren‹ und ›Würmer‹ als im Sommer des Vorjahrs. »Damit Eindringlinge kein gar so leichtes Spiel haben, braucht man schon eine robuste Tür mit einem stabilen Schloss«, so Carle weiter. Im Fachjargon heißt eine solche Tür *Firewall*. Sie kann ein spezielles Alarmsystem oder ein zusätzlich vorgeschalteter Rechner sein.

Immer raffiniertere Netzattacken lassen herkömmliche Sicherungssysteme – wie zum Beispiel Anti-Viren-Programme – alt aussehen. Der Internet-Wurm *Blaster* hat innerhalb von acht Tagen Kosten in Höhe von zwei Millionen US-Dollar verursacht. Der Wurm *Welchia* legte neun Stunden lang eine Internetseite des US-Außenministeriums für die Vergabe von Visa lahm.

Ein Angriffspunkt ist der Aufbau der Internetverbindung, bevor Inhalte übertragen werden: Bei einer so genannten *Distributed Denial-of-Service-Attack* (DDoS) werden pro Sekunde mehrere Hundert oder mehrere Tausend solcher Anfragen an einen Rechner oder Server gestellt. Weil das ›Opfer‹ diese Anfragen irgendwann nicht mehr verarbeiten kann, bricht es unter dieser Bombardierung zusammen und verweigert seinen Dienst. Die Angreifer verwenden für eine solche Attacke nicht eigene Rechner, sondern kapern über zuvor verbreitete Schädlinge Rechnersysteme in aller Welt. Damit bauen sie systematisch Datenmüllkanonen auf. Neben der simplen Überflutung gibt es aber noch kreativere Tricks: Zum Beispiel lassen gefälschte Absenderadressen einen Rechner bei der Fehlersuche ins Leere laufen. Häufig sind Angriffe nur schwer von berechtigten Anfragen zu unterscheiden.

Bei der Analyse finden die Computer-Experten jedoch typische Muster in den übertragenen Daten, die alle Vorgänge dokumentieren. »Man kann dies mit einem verräterischen Fingerabdruck vergleichen, den auch ein Einbrecher hinterlassen würde«, so Carle. Mittels mathematischer Verfahren versuchen die Tübinger, solche Fingerabdrücke aufzuspüren. Mit ihrer Hilfe hoffen sie, intelligente Systeme entwickeln zu können, die das Netz auch gegen heute noch unbekannte Attacken wappnen.

Bislang muss man schon vorher wissen, wie ein ›Schädling‹ aussieht, um ihm nicht wehrlos ausgeliefert zu sein. So hinkt man den Angreifern ständig hinterher. Die *Diadem-Firewall* soll auch neuartige Strategien von ›Schädlingen‹ selbstständig erkennen. Entdeckt das System eine Häufung an sich unverdächtiger Vorgänge, könnte sich ein mehrstufiger *DDoS-Angriff* zusammenbrauen. Wie bei einer Rasterfahndung gilt es daher, ständig Datensätze zu durchkämmen, zu sortieren und zu überprüfen. Um den Angreifern immer einen Schritt voraus zu sein, verbinden die Forscher zahlreiche intelligente *Firewalls* miteinander, die sich bei jedem Verdacht sofort gegenseitig warnen können.

Schon in zwei Jahren wollen die Netzbetreiber von der Französischen und Polnischen Telekom den ersten Prototyp des neuen intelligenten Abwehrsystems testen. Eines Tages soll das Internet so zuverlässig sein, dass nicht einmal für Notrufe andere Netze nötig wären. »Das Internet könnte sogar das gute alte Telefonnetz ersetzen, wenn wir es schaffen, eine intelligente Abwehr zu entwickeln«, mutmaßt Carle. Dann wird die Vision der Diadem-Fahnder von einem sicheren Netz Wirklichkeit. OTZ

www.diadem-firewall.org