Virenscanner haben noch Schwächen

Hacker kommt nach 20 Minuten ins Netz

Einem Großteil der Internetgefahren kann man mit heutigen Mitteln begegnen. Dennoch gibt es in Sachen IT-Sicherheit noch einiges zu tun, zeigt eine Forschertagung.

„Webserver sind im Internet ein primäres Angriffsziel", zieht Ulrich Flegel von der Uni Dortmund ein Fazit des Security-Treffens Dimva, das von der Fachgruppe Sidar der Gesellschaft für Informatik (GI) mitveranstaltet wurde (www.gi-fg-sidar.de/dimva2004). Insbesondere Microsoft steht im Visier: 95 Prozent aller Webserver-Angriffe zielen auf deren Internetsoftware IIS. „Diese muss man also besonders sorgfältig absichern", rät Flegel. Schließlich zeigt die Auswertung elektronischer Köder wie Honeypots und Sensornetze, dass IT-Systeme im Mittel 20 Minuten nach dem Anschluss ans Internet angegriffen werden. Meist werden dabei mehrere Exploits automatisiert durchprobiert. Immerhin: 90 Prozent dieser Angriffe lassen sich mit bekannten Mitteln wie Firewalls und Patchen abwehren, so Flegel.

Doch gibt es noch genug Security-Baustellen. So wurde in Dortmund deutlich, dass selbst bei gehärteten Betriebssystemen die Möglichkeiten der Angreifer zwar eingeschränkt, die Rechner aber nach wie vor verwundbar sind. Zudem zeigen Tests, dass Virenscanner weiter Erkennungsschwierigkeiten bei komprimierten Dateien haben. Und auch das Aufspüren von Hintertüren (so genannten Rootkits) bleibt schwierig.

Allerdings wurden auf der Security-Tagung nicht nur Probleme, sondern vor allem Lösungen für heraufziehende Bedrohungsszenarien vorgestellt – etwa für komplexe, föderierte IT-Verbünde via Webservices oder mobile Ad-hoc-Netze. *ab*