Diebstahlschutz für virtuelle Maschinen

Wissenschaftler der TU Darmstadt haben einen Weg gefunden, Hacker-Attacken auf virtuelle Maschinen frühzeitig zu erkennen. Unternehmen und Behörden, die virtuelle Maschinen einsetzen, können die dort gespeicherten Daten so vor Diebstahl schützen. Virtuelle Maschinen sind Computer, die keinerlei Hardware-Komponenten enthalten, sondern vollständig von einer Software simuliert werden. Das birgt allerdings auch ein Risiko: Der Nutzer merkt nämlich nicht, wenn eine virtuelle Maschine bei einem Hacker-Angriff illegal aus dem jeweiligen Firmen- oder Behörden-Netz heraus verschoben wird. In wenigen Sekunden kann so ein gesamter Rechner mit allen gespeicherten Daten in falsche Hände geraten.

Der Diebstahl kann jedoch verhindert werden, wenn die Bewegung der Maschine rechtzeitig bemerkt wird. Ein solches Frühwarnsystem entwickelte das Darmstädter Forscherteam. Dabei machen sich die Wissenschaftler die Echoanfrage-Funktion zunutze, das so genannte „Anpingen". „Beim Umzug einer virtuellen Maschine sind einzelne Informationspakete länger im Netz unterwegs und gehen teilweise sogar verloren. Eine virtuelle Maschine in Bewegung sendet also ein spezifisches Echomuster aus", erklärt André König von der TU. Abhilfe soll nun eine Software schaffen, die dieses spezifische Echomuster erkennt und Schutzmaßnahmen gegen den Angriff auslöst. Wichtig sei dabei vor allem der Faktor Zeit, betont König: „Daten, die einmal entwendet sind, lassen sich nicht mehr zurückholen – der Angriff muss daher vor der vollständigen Migration der Maschine erkannt und gestoppt werden." -sg-

Technische Universität Darmstadt, Darmstadt
Tel. 06151/16-2750, www.tu-darmstadt.de