Echo verrät Datenklau

TU Darmstadt entwickelt Diebstahlschutz für virtuelle Maschinen

Wissenschaftler der TU Darmstadt haben einen Weg gefunden, Hacker-Attacken auf virtuelle Maschinen frühzeitig zu erkennen. Damit können Unternehmen und Behörden, die virtuelle Maschinen einsetzen, die dort gespeicherten Daten vor Diebstahl schützen.

Virtuelle Maschinen sind Computer, die keinerlei Hardware-Komponenten enthalten, sondern vollständig von einer Software simuliert werden. Im Vergleich zu herkömmlichen Computern sind sie deutlich flexibler und effizienter einsetzbar, weil sie sich – wie alle anderen Softwaredateien auch – schnell und ohne großen Aufwand von einem zum anderen Ort verschieben lassen. Das birgt allerdings ein Risiko: Der Nutzer merkt nicht, wenn eine virtuelle Maschine bei einem Hacker-Angriff illegal aus dem jeweiligen Firmen- oder Behördennetz herausgeschoben wird. In wenigen Sekunden kann ein gesamter Rechner mit allen gespeicherten Daten in falsche Hände geraten.

Schnelle Reaktion gefordert

Wird die Bewegung der Maschine rechtzeitig bemerkt, kann der Diebstahl verhindert werden. Ein solches Frühwarnsystem entwickelt derzeit das Forscherteam um Dr. André König vom Fachgebiet Multimedia Kommunikation (KOM) des Fachbereichs Elektrotechnik und Informationstechnik. Dabei machen sich die Wissenschaftler die Echoanfrage-Funktion zunutze, das sogenannte „Anpingen“. „Eine virtuelle Maschine in Bewegung sendet ein spezifisches Echomuster aus“, erklärt König. Die Forscher entwickeln nun eine Software, die dieses 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.“