Diebstahlschutz für virtuelle Maschinen

DA E
02.09

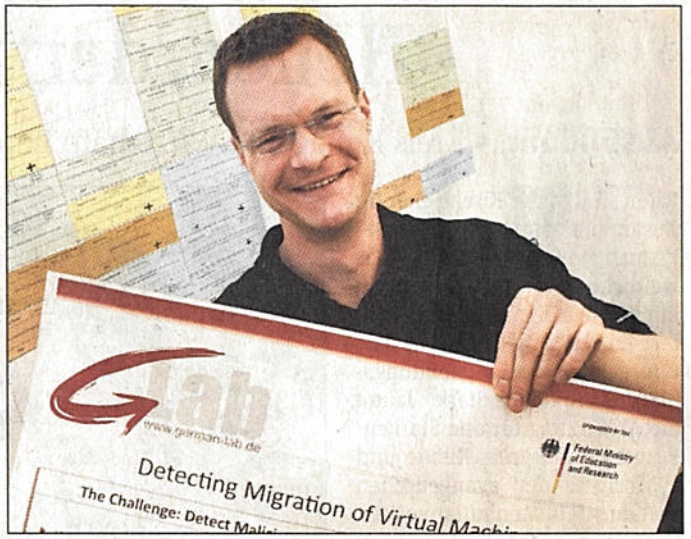
Multimedia Kommunikation – TU-Forscher entwickeln ein Frühwarnsystem für ungewollte Datenbewegungen

VON STEFFEN HUSS

Auf einer Rangliste der am meisten diskutierten IT-Begriffe dürfte der Ausdruck „Cloud Computing" derzeit ziemlich weit oben stehen. Dahinter steckt eine ganz einfache Idee: Die meisten Unternehmen dimensionieren ihre Rechenleistung so, dass auch zu Spitzenzeiten keine Probleme auftreten. Amazon zum Beispiel hat zu Weihnachten rund zehn Mal mehr Zugriffe auf die Webseite als in umsatzschwächeren Zeiten. Diesem Ansturm müssen die Server zuverlässig standhalten. Die Folge: Im restlichen Jahr gibt es riesige Überschusskapazitäten – eine gigantische Verschwendung.

Cloud Computing ist der Versuch, diese nicht benötigte Rechenleistung anderen Nutzern zugänglich zu machen und zu verkaufen. Mit den Sicherheitsproblemen, die in der Rechnerwolke auftreten können, beschäftigen sich aktuell auch Forscher der TU Darmstadt. Einer von ihnen ist André König. „Man kann das vergleichen mit einem Mehrparteien-Haus", erklärt er. „Ein solches Haus kann man in verschieden große Wohneinheiten unterteilen."

Ähnlich läuft es beim Cloud Computing: Die Überschusskapazitäten eines großen Rechenzentrums, zum Beispiel von Amazon, werden in viele kleine Einheiten unterteilt, die dann vermietet werden können. Diese Einheiten heißen virtuelle Maschinen. Der Zugriff darauf kann auch vom eigenen Computer aus erfolgen, und die virtuellen Maschinen funktionieren auch wie ein ganz normaler Computer – nur dass die Hardware dazu eben in einem Rechenzentrum steht.



Findiger Forscher: André König hat einen Weg gefunden, Hacker-Attacken auf virtuelle Maschinen frühzeitig zu erkennen. FOTO: ROMAN GRÖSSER

Die Software, die die große Rechenleistung des Anbieters in kleinere virtuelle Maschinen organisiert, heißt Hypervisor. Sie simuliert die Hardware eines normalen Rechners. Wie überall im IT-Bereich können auch in der Rechnerwolke Sicherheitsprobleme auftreten.

Eine besonders kritische Phase ist die so genannte Migration. Diese findet zum Beispiel dann statt, wenn eine virtuelle Maschine innerhalb des Rechenzentrums von einem Server auf einen anderen verschoben wird, um die Last besser zu verteilen. Sie geschieht bei laufendem Betrieb, der Nutzer merkt davon im Normalfall nichts. „Wenn es jemandem gelingt, den Hypervisor anzugreifen und damit die Migration auszulösen, dann kann er die virtuelle Maschine entführen", erläutert König. Der User muss damit rechnen, dass sämtliche sensible Daten seiner virtuellen Maschine vom Angreifer ausgelesen werden.

Verräterische Pings

Für genau dieses Problem möchte André König einen Diebstahlschutz finden. Er will von außen erkennen, ob eine Migration stattfindet. Wird rechtzeitig eine Migration erkannt, die nicht vom Rechenzentrum geplant wurde, kann der Prozess gestoppt werden. Seine Grundidee: Während des Migrationsprozesses ist die virtuelle Maschine beschäftigt und braucht so ein wenig länger, um Anfragen zu beantworten. Deshalb bombardiert König die virtuelle Maschine fortlaufend mit mehreren Anfragen (Pings, auch bekannt aus U-Boot-Filmen) pro Sekunde, die von dieser reflektiert werden. Während des etwa zehn Sekunden andauernden Migrationsprozesses brauchen die Antworten tatsächlich rund zehn bis zwanzig mal länger.

Das Problem: Diese Verzögerungen können auch durch andere Faktoren wie plötzliche höhere Auslastung zu Stande kommen. „Wir haben uns daher gefragt: Gibt es in den Verzögerungen während des Migrationsprozesses ein charakteristisches Muster?", berichtet André König. Tatsächlich konnte eine solche Signatur gefunden werden – allerdings nur unter den kontrollierten Bedingungen des TU-Rechenzentrums.

Hier liegt für die Forscher ein weites Themenfeld. Die nötige Förderung vorausgesetzt, möchte man an der TU untersuchen, ob eine solche Signatur auch noch identifiziert werden kann, wenn größere Netzwerke betrachtet werden. Dann nämlich ist die Entfernung für die gesendeten Pings deutlich länger, die Anfragen laufen über mehrere Router, das Muster wird verzerrt. „Je allgemeiner wir ein charakteristisches Muster der Antworten beschreiben können, desto besser ist die Methode anwendbar", sagt André König. Cloud Computing dürfte also auch in der Forschung weiterhin viel diskutiertes Thema bleiben.

VORSCHAU

Die nächste Hochschulseite erscheint am Freitag, 7. Oktober.