

Dem Datendiebstahl im Internet auf der Spur

Sony, Google und Apple, CIA, IWF und der US-Senat – fast täglich werden Unternehmen und Behörden Opfer von Hackerangriffen. Auch in Regierungskreisen wird die Bedrohung im Internet mittlerweile als ernst eingeschätzt. Erst Anfang des Jahres wurde das Nationale Cyber-Abwehrzentrum gegründet, das seit April den Kampf gegen die Kriminalität im Netz aufgenommen hat. Einen Angriffspunkt für Hacker bieten insbesondere virtuelle Maschinen, die z. B. beim Cloud Computing benutzt werden.

Bei den virtuellen Maschinen handelt es sich um Computer, die keinerlei Hardwarekomponenten enthalten, sondern die vollständig von einer Software simuliert werden. Eine virtuelle

Maschine verfügt über alle Bestandteile eines physisch existenten Rechners wie Motherboard, VGA-Karte, LAN-Karte, Festplatten, CPU, Ram-Module. Für den Nutzer ist nicht unterscheid-

bar, ob er auf einer virtuellen Maschine oder einem realen Rechner arbeitet.

Anstelle einer Vielzahl einzelner realer Rechner können mehrere virtuelle Maschinen auf einem einzigen leistungsstarken Server gleichzeitig parallel betrieben werden. Die Ressourcen eines Servers können so effizient unter mehreren virtuellen Maschinen aufgeteilt und genutzt werden. Immer mehr Unternehmen betreiben deshalb aus Kostengründen heute schon keine eigene IT-Infrastruktur mehr, sondern mieten bei großen Dienstleistern wie Amazon oder Google virtuelle Maschinen an.

Wie jede andere Softwaredatei lassen sich virtuelle Maschinen zudem ohne großen Aufwand von einem Ort bzw.

Server an einen anderen Ort verschieben und garantieren den IT-Dienstleistern damit jederzeit eine optimale Ressourcenauslastung. Die Migrationen können innerhalb weniger Sekunden im laufenden Betrieb vorgenommen werden, ohne dass der Nutzer hiervon Kenntnis nimmt. „Diese Eigenschaft gewährleistet die Grundfunktion virtueller Maschinen, öffnet zugleich aber dem Datenklau im Internet Tür und Tor“, gibt Prof. Ralf Steinmetz zu bedenken. Denn der Nutzer merke auch dann nichts, wenn eine virtuelle Maschine illegal aus dem Netz heraus verschoben wird. In wenigen Sekunden

kann so ein gesamter Rechner mit allen gespeicherten sensiblen Daten in die falschen Händen geraten.

Am Lehrstuhl von Prof. Steinmetz entwickelt ein Forscherteam um Dr. André König eine Methode, mit der sich die Migration von virtuellen Maschinen

Kontakt:

*Dr.-Ing. André König, TU Darmstadt,
Fachgebiet Multimedia Kommunikation,
Rundeturmstr. 10, 64283 Darmstadt,
Tel.: 061 51/16-61 37 Fax: -61 52,
E-Mail: Andre.Koenig@kom.tu-darmstadt.de*

frühzeitig aufspüren lässt. Zu Nutzen machen sie sich hierbei die Echoanfragefunktion, das sogenannte Anpingen. „Beim Umzug einer virtuellen Maschine sind einzelne Informationspakete länger im Netz unterwegs und gehen teilweise sogar verloren. Hieraus ergibt sich ein ganz spezifisches Echomuster, das wir mit der von uns programmierten Software identifizieren“, erklärt A. König. Das Ganze sei jedoch ein Wettlauf mit der Zeit. Entscheidend ist, dass ein Angriff vor der vollständigen Migration entdeckt wird. Denn Daten, die einmal entwendet sind, lassen sich nicht mehr zurückholen. ■