Dem Datendiebstahl im Internet auf der Spur

Spezifisches Echo-Muster verrät ungewollte Datenbewegungen

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 gründete die Bundesregierung das Nationale Cyber-Abwehrzentrum, das seit April den Kampf gegen die Kriminalität im Netz aufgenommen hat. Einen Angriffspunkt für Hacker bieten insbesondere virtuelle Maschinen, die beispielsweise im Bereich des Cloud Computings eingesetzt werden. Forscher am Fachgebiet Multimedia Kommunikation der Technischen Universität Darmstadt haben ein Verfahren gefunden, mit dem sie Attacken auf virtuelle Maschinen rechtzeitig erkennen und so den Datenklau verhindern können.

Moderne IT-Anwendungsszenarien wie das Cloud Computing basieren auf sogenannten virtuellen Maschinen. Hierbei handelt es sich um Computer, die keinerlei Hardwarekomponenten enthalten, sondern vollständig von einer Software simuliert werden. Eine virtuelle Maschine verfügt über alle Bestandteile eines physisch existenten Rechners wie Motherboard, VGA-Karte, Netzwerkkarte, Festplatten, CPUs, Ram-Module. Für den Nutzer ist nicht unterscheidbar, 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 maximal 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 Dienstanbietern wie Amazon oder Goggle 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-Dienstanbietern 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 Grundfunktionalität virtueller Maschinen, öffnet zugleich aber dem Datenklau im Internet Tür und Tor“, gibt Professor 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 frühzeitig aufspüren lässt. Zu Nutze 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 an ganz spezifisches Echomuster, dass wir mit der von uns programmierten Software identifizieren“, erklärt König. Das Ganze sei jedoch ein Wettlauf mit der Zeit. Entscheidend ist, dass ein Angriff vor der vollständigen Migration entdecket wird. Denn Daten, die einmal entwendet sind, lassen sich nicht mehr zurückholen.

Pressekontakt:

Dr.-Ing. André König
Technische Universität Darmstadt
Fachgebiet Multimedia Kommunikation
Rundeturmstr. 10, 64283 Darmstadt
Telefon: 06151 16-6137
Fax: 06151 16-6152
E-Mail: Andre.Koenig@kom.tu-darmstadt.de