

Generell gewinnen Unternehmen durch Virtualisierung aber an Schutz



Vmware-Bugs bieten Angriffspunkte für Hacker

Von Von Armin Barnitzke

26. September 2007

Die kürzlich von Vmware geschlossenen Sicherheitslücken verdeutlichen, dass Virtualisierungsansätze durchaus Risiken bergen. Allerdings stärkt die Virtualisierung in der Regel auch die Sicherheit von PCs und Servern – Firmen müssen daher Nutzen und Risiken stets abwägen.

Insgesamt 20 zum Teil kritische Löcher musste Vmware in Produkten wie ESX Server, Vmware Server, Vmware Workstation, Vmware ACE oder Vmware Player stopfen. [Drei davon](#) fanden Forscher von IBMs ISS-Security-Team Xforce im integrierten DHCP-Server (Dynamic Host Configuration Protocol), der sich um die dynamische Zuweisung von IP-Adressen kümmert. Über diese Bufferoverflow-Schwächen könne ein Angreifer aus einer virtuelle Maschine ausbrechen und die Kontrolle über den gesamten Server übernehmen, berichtet ISS.

„Ja, da droht Gefahr“, bestätigt Security-Experte Stefan Strobel, „der Ausbruch aus einem Gastsystem auf den Host ist eigentlich der GAU.“ Allerdings müsse man das Ganze auch relativieren, so Cirosec-Chef Strobel: „Damit ein Angreifer aus einem Gast ausbrechen und den Host entern kann, muss er erst einmal die Gast-Applikation unter seine Kontrolle gebracht haben. Der Ausbruch ist erst der zweite Schritt.“ Daher werde jetzt nicht jeder Vmware-Anwender direkt wegen diesen Bugs angreifbar. „Nur wird eben die zusätzliche Schutzschicht unterhöhlt.“

Und Strobel rechnet durchaus noch mit weiteren Schwachstellen ähnlicher Art. Insgesamt sei es aber einfacher, eine Virtualisierungssoftware sicher zu machen als etwa ein Betriebssystem – daher erwartet er keine Bug-Schwemme. Zudem hat sich Vmware neulich erst mit dem Intrusion-Prevention-Spezialisten [Determina verstärkt](#), der Bufferoverflows automatisch unterbinden kann, egal ob im Hypervisor selbst oder in der Gast-Applikation.

Unabhängig davon befeuern die entdeckten Schwachstellen die Debatte, ob Virtualisierung nun der Sicherheit nutzt oder schadet. So zeigt eine Forrester-Umfrage unter 137 Security-Profis durchaus noch Klärungsbedarf. Manche Sicherheitsbeauftragte sind sich über die Auswirkungen der Virtualisierung auf die IT-Security noch nicht ganz im Klaren, andere sehen Probleme beim Management von virtuellen Servern oder haben Zweifel an der Reife der Technologie. Oder sie fühlen sich generell unbehaglich, wenn etwas noch unterhalb des Betriebssystems werkelt.

Solche Befürchtungen („Bin ich in der realen Welt oder in der Matrix?“) haben etwa Forschungen über Rootkit-Trojaner wie Vitriol, Subvirt Oder Blue Pill geweckt. Diese nutzen Intels Virtualisierungsfunktionen, um sich auf einem befallenen System unter das Betriebssystem zu schieben und dann dort von der PC-Antivirensoftware quasi nicht entdeckbar ihr

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Unwesen zu treiben (mehr [hier](#) und [hier](#))

Allerdings beruhigt Strobel: „Ganz so einfach ist es ja dann doch nicht, wie man jüngst auf Hacker-Konferenzen sehen konnte. Ein Virtualisierungs-Rootkit so zu schreiben, dass es wirklich nicht erkennbar ist, stellt sich als recht schwierig heraus“. Zudem: Die Virtualisierungsfunktionen der modernen CPUs werde man nicht mehr entfernen können. Damit sei das Ganze keine Argument gegen Vmware, sondern eher ein Feature von CPUs, das für gute und schlechte Zwecke verwendet werden kann.

Auch das Argument des schwierigen Managements und etwa Patches virtueller Maschinen will Strobel nicht stehen lassen: Mit einem geeignetem Patch-Management von Bigfix oder Patchlink sei das Ganze gar kein Problem. Durch die Virtualisierung und Trennung der Aufgaben werde zudem das Patchen einfacher. „Es gibt weniger Abhängigkeiten innerhalb einer Maschine und durch ein Rollback der Virtualisierung kann man besser mit Fehlern umgehen.“

Auch das Testen von Patches wird durch Virtualisierung einfacher und kostengünstiger, weil die IT-Abteilung dann nicht für jedes Produktivsystem ein vollständiges Duplikat vorhalten muss, ergänzen die Analysten von Forrester. Zudem könne man gehackte oder mit Trojanern verseuchte Rechner sehr schnell und einfach wieder in den Original-Zustand zurück versetzen.

Und natürlich lassen sich über Virtualisierung Anwendungen und Prozesse auf einem Rechner von einander trennen, so dass ein Angreifer zwar etwa via Exploit eine Browser-Schwachstelle ausnutzen kann, aber dann in der virtuellen Maschine eingesperrt bleibt – es sei denn, er kann zum Ausbruch Schwachstellen im Hypervisor selbst nutzen.

Strobel: „Aus Sicherheitssicht muss man in solchen Fällen abwägen, wie der Zustand vorher zu bewerten ist und was man durch die Virtualisierung erreicht“. Als Faustformel nennt er:

Wenn ich vorher alle Applikationen auf einem gemeinsamen Server hatte und durch die Virtualisierung eine Trennung erreiche, dann gewinne ich dabei Sicherheit.

Wenn ich aber vorher einzelne Server hatte und diese per Virtualisierung etwa auf einen gemeinsamen ESX-Server bringe, verliere ich etwas Sicherheit. Gleichzeitig gewinne ich aber auch an Kontrolle. „Die Antwort ist dann nicht ganz einfach. Das läuft also auf eine Risikoanalyse hinaus.“

Computerzeitung.de 26.09.07