Dirk Fox

Hypervisor

Hintergrund

Unter einem Hypervisor wird ein Programm verstanden, das eine virtuelle Betriebsumgebung für andere Programme bereitstellt. Eine solche „virtuelle Hardware" hat zahlreiche Vorteile gegenüber einem Betrieb ohne Virtualisierung:

- *Bessere Nutzung leistungsfähiger IT-Systeme*: Auf einer Hardware, beispielsweise einem Server, können mehrere „virtuelle Maschinen" gleichzeitig betrieben und die verfügbare Leistung so besser ausgelastet werden; dabei sinkt zugleich der Energiebedarf.
- *Höhere Verfügbarkeit*: Stürzt eine virtuelle Maschine durch einen Programmfehler ab, so sind davon Programme in anderen virtuellen Maschinen auf derselben Hardware in der Regel nicht betroffen.
- *Schnellerer Wiederanlauf*: Wird eine virtuelle Maschine von Zeit zu Zeit gespeichert, kann sie bei einem Fehler oder Absturz einfach wieder eingespielt werden – ein Neustart des abgestürzten Systems ist nicht erforderlich.
- *Einfacher Hardware-Wechsel*: Soll an einem PC oder Server die Hardware getauscht werden, kann die virtuelle Maschine weiter genutzt werden, ohne dass eine neue Installation oder Umkonfiguration erforderlich wäre.
- *Ressourcen-Kontrolle*: Der Zugriff auf Ressourcen des Systems (Netzwerk, Speicherbereiche, Peripheriegeräte wie Drucker etc., Speichermedien) wird vom Hypervisor kontrolliert; dort werden die Berechtigungen zentral organisiert.
- *Sicherheitsgewinn*: Schadprogramme wie Viren oder Würmer, die eine virtuelle Maschine befallen, sind in ihrer Wirkung in der Regel auf die jeweilige virtuelle Maschine beschränkt und können nicht auf parallele virtuelle Systeme übergreifen.

Der Gewinn an Sicherheit und Flexibilität wird dabei im Wesentlichen durch eine verringerte Betriebsgeschwindigkeit erkauft, da alle Zugriffe auf Speicher, Netzwerk, Hardware oder angeschlossene Geräte über den Hypervisor erfolgen und die Ressourcen (verfügbarer Arbeitsspeicher, Prozessorleistung) mit den auf derselben Hardware betriebenen virtuellen Maschinen geteilt werden.

Das Konzept ähnelt im Prinzip dem Sicherheits-Manager des „Sandbox"-Modells [1], das die Firma Sun Microsystems Inc. Mitte der 90er Jahre für Java entwickelte. Java-Programme laufen darin in einer „Java Virtual Machine" (JVM) ab. Der Zugriff auf Ressourcen wird während der Codeausführung kontrolliert. Daher sind Angriffe über Java-Code schwierig und in ihrer Wirkung begrenzt. Das Sandbox-Modell ist jedoch auf Java-Programme beschränkt, während ein Hypervisor ein komplettes IT-System „simuliert".

Verbreitung

Seit einigen Jahren bieten mehrere Hersteller Hypervisoren an. Damit betriebene virtuelle Maschinen spielen vor allem in Rechenzentren schon heute eine zentrale Rolle. Das verdanken sie insbesondere ihrer Eigenschaft, leistungsfähige Server geeignet auszulasten und bei Ausfällen schnell wieder in Betrieb genommen werden zu können. Auch das Einrichten eines neuen Systems erfordert bei Verwendung vorbereiteter Standard-Systeme nur minimalen Aufwand.

Im Bereich der Endsysteme werden Hypervisoren zunehmend eingesetzt, um die Rechenleistung von Clients auf zentrale Server zu verlagern: Damit wird die Verwendung von so genannten *thin clients* möglich, Systemen ohne eigene Festplatte und mit vergleichsweise geringer Prozessorleistung, indem die virtuelle Maschine auf einem Server betrieben wird.

Sicherheit

Hypervisoren müssen gegen zweierlei Arten von Angriffen geschützt werden: Einerseits vor Versuchen von außen, das System zu manipulieren oder zu übernehmen, und andererseits gegen Angriffe aus einer virtuellen Maschine mit dem Ziel, den Hypervisor oder parallel betriebene virtuelle Systeme ebenfalls zu infizieren.

Beide Schutzziele sind in der Praxis einfacher zu erreichen als der Schutz bspw. eines kompletten Betriebssystems, da der Hypervisor selbst nur eine einzige Anwendung darstellt und daher z. B. nicht vor Angriffen über einen Browser geschützt werden muss. Zudem werden Daten an und von Schnittstellen nur durchgereicht, aber nicht verarbeitet.

Zwar wurden gelegentlich einzelne Sicherheitslücken von Hypervisoren entdeckt und publiziert; sie waren aber nur mit viel Aufwand praktisch ausnutzbar und wurden zudem schnell geschlosssen.

Ausblick

Mit der weiteren Leistungszunahme von PC- und Server-Hardware werden Hypbervisoren in naher Zukunft auch auf stationären Endsystemen die Regel sein, da sie bei einer zentralen Speicherung der virtuellen Maschine eine erheblich vereinfachte Wartung (Updates, Konfigurationen etc.) erlauben.

Sie bieten zudem die Chance, angreifbare Anwendungen wie den Internet-Zugang in von anderen, sicherheitskritischen Anwendungen getrennten virtuellen Maschinen zu betreiben, sodass sich der Schaden bei einem erfolgreichen Angriff begrenzen lässt. Zudem lassen sich sicherheitskritische Anwendungen mit geringeren Berechtigungen betreiben – z. B. ein Online-Banking ohne Schreibrechte im System –, sodass bestimmte Angriffsarten wie zum Beispiel Trojaner, die erweiterte Berechtigungen für die Ausführung des Schadcodes benötigen, ausgeschlossen werden können.

Literatur

[1] Fox, Dirk: Sandbox-Modell. Gateway, DuD 2/1998, S. 96.