Netzwerksicherheit im Virtual Machine Live Migration Umfeld

Studiengang: MAS Information Technology
Betreuer: Markus Pfluger (BIT)
Experte: Prof. Rolf Lanz

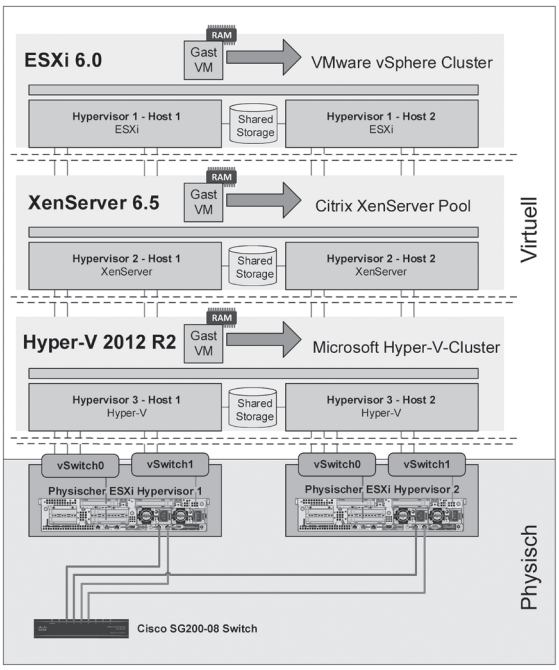
Ein zentrales Element bei Cloud-Lösungen ist der Hypervisor. Er besitzt die Fähigkeit, die auf ihm ausgeführten virtuellen Maschinen, über das Netzwerk, auf einen andern Hypervisor zu migrieren. Diese Arbeit untersucht, wie sicher die Daten bei einer VM Live-Migration übertragen werden und wie allfällige Mängel zu beheben sind.

Umfeld

Im Umfeld der Bundesverwaltung werden mehrere tausend virtuellen Maschinen (VMs) auf einem Hypervisor Produkt betrieben. In der öffentlichen Verwaltung stellen sich IT-Lösungen regelässig WTO Ausschreibungsverfahren. Es kann sein, dass ein verwendetes Hypervisor Produkt nach einer Ausschreibung ersetzt werden muss. Um darauf vorbereitet zu sein, soll die Sicherheit im Bereich VM Live Migration Netzwerk auf den im Markt verbreiteten Produkten geprüft werden.

Problemstellung

Im Falle einer VM Live Migration wird der gesamte Arbeitsspeicher der VM über das Netzwerk übertragen. In diesen Daten sind unter anderem kryptografische Schlüssel enthalten, mit denen eine aufgezeichnete und verschlüsselte Datenübertragung nachträglich entschlüsselt werden kann. Ziel dieser Arbeit ist es zu prüfen, wie der Arbeitsspeicher einer VM zwischen zwei Hypervisoren übertragen wird. Weiter soll aufgezeigt werden, wie das Netzwerk bestmöglich geschützt werden kann und mit welchen technischen Einschränkungen man dadurch rechnen muss.



Übersicht Laborumgebung mit Nested-Hypervisor Installationen

Vorgehen

Es wurde eine Laborumgebung mit den verbreiteten Hypervisor-Produkten aufgebaut und diese auf deren Sicherheit im Bereich der VM Live Migration überprüft. In einem zweiten Schritt wurde das VM Live Migration Netzwerk mittels einer IPsec Implementation abgesichert und Performance Messungen durchgeführt. Die anschliessende Analyse der Messergebnisse soll Aufschluss darüber geben, ob durch die zusätzlichen Sicherheitsmassnahmen (signifikante) zeitliche Verzögerungen im VM Live Migrationsvorgang entstehen.

Resultate

Die Analyse der Labormessungen ergab, dass der Arbeitsspeicher der migrierten VMs standardmässig unverschlüsselt über das Netzwerk übertragen wurde. Als Folge daraus konnten kryptografische Schlüssel ausgelesen werden.

Die aufgezeichneten Performance Messungen zeigten, dass sich die Zeitdauer einer VM Live Migration durch das Verschlüsseln mit IPsec im Maximalfall um den Faktor 3 vergrösserte.

Fazit

Betreiber von Virtualisierungs-Lösungen sollten sich mit der Absicherung des VM Live Migration Netzwerks auseinandersetzen. Insbesondere, wenn geplant ist, VMs im laufenden Betrieb über die Grenzen eines Rechenzentrums hinweg zu migrieren.

Am effizientesten geschieht dies mit Lösungen, die auf OSI Layer 2 Technologien basieren. Diese weisen allerdings oft den Nachteil auf, dass sie die Daten nicht End-to-End sondern nur Hop-to-Hop verschlüsseln können. Aus diesem Grund sollten auch OSI Layer 3 Technologien, wie IPsec ins Auge gefasst werden.

Hanspeter Locher