Sicherheit in VMwares Infrastructure 3

# Riegel vorgeschoben

**Christoph Puppe**

VMware ist mit Infrastructure 3 führend in x86er-Server-Umgebungen. Da jede Software Angreifer anlocken kann, sollte man beim Einrichten der Server besonders sorgfältig zu Werke gehen und die Schwachstellen schützen.

Virtualisierung erfreut sich vor allem im Serverbereich zunehmender Beliebtheit, was sicherlich mit an der gestiegenen Leistungsfähigkeit und den großen Speichervolumina heutiger Systeme liegt. Doch gerade, wenn es um zentrale Dienste der IT in Unternehmen geht, sind wirksame Schutzmaßnahmen gefragt. Dabei gibt es einige Unterschiede zwischen physischen und virtuellen Servern.

In einer virtuellen Umgebung legen die physischen Hosts und deren Verwaltungsdienste das Fundament für das Sicherheitskonzept. In „VMwares Infrastructure 3" (VI3) [1] stehen vier Komponenten im Mittelpunkt: der ESX Server, die Datenbank für die Konfigurationseinstellungen, das Managementmodul „Virtual Center" (VC) sowie der Arbeitsplatz mit dem Verwaltungs-Client. Das Herzstück, der VMkernel, muss vor allem gegen Angriffe geschützt sein. Um die Sicherheit seiner Virtualisierungslösung unter Beweis zu stellen, hat VMware nach eigenen Aussagen einen Sourcecode Audit unternommen und mit positiven Zitaten der Prüfer geworben.

Ausschlaggebender sind die international gültigen „Evaluation Assurance Level" (EAL – siehe Onlinequellen [a]). Die vorige Version (ESX 2.5, VC 1.2.0) war für EAL 2 zertifiziert, die aktuelle (ESX 3.01 und VC 2.0.1) ist derzeit für EAL4+ in Vorbereitung. Es gibt laut Definition sieben Stufen. Sie sind jedoch kein Maßstab für die Sicherheit, sondern beschreiben ausschließlich die Ebene, auf der ein System im Test die Anforderungen seines „Protection Profile" (PP) [b] erfüllt hat. PP folgt dem Evaluierungsprozess der Common Criteria [c].

Eine deutlichere Sprache als die Zertifizierungen und Ausführungen in den Whitepapers des Herstellers sprechen Veröffentlichungen über die Verwundbarkeit der Komponenten. Darunter ist bisher nur eine zu finden, die es einem Angreifer von einer virtuellen Maschine (VM) aus erlaubt hätte anzugreifen [d]. Allerdings nur unter der Bedingung, dass eine saubere Trennung der VMs untereinander und von der Infrastruktur stattgefunden hat. Und von den bedrohlichen Rootkits [2] gab es bis dato nur Laborversionen.

## Architektur der VI3: Linux als Pförtner

Das eigentliche Arbeitspferd, der ESX Server – im Folgenden einfach als ESX bezeichnet – startet mit einem angepassten Linux von Red Hat, das es als Boot-Loader für den VMkernel nutzt. ESX läuft nicht auf einem Linux-Kernel, sondern enthält einen eigenen, der als Erstes das „Console Operating System" (COS) bootet. Es bietet eine Shell, diverse CLI-Befehle, die Daemons zur Verwaltung (*authd*, *hostd*) und eine Weboberfläche auf Basis von Apache sowie Tomcat. Die Authentifizierung beim COS erfolgt über die von Linux bekannten Mechanismen samt der Anbindung an ein Active Directory per PAM.

Der Administrator nutzt hauptsächlich den VI-Client, eine Windows-Anwendung, die er auf seinem Arbeitsplatz installieren muss. Sie erlaubt die Konfiguration fast aller Funktionen der VI3. Der VI-Client verbindet sich per SSL entweder direkt mit ESX oder mit einem Management-Server, dem Virtual Center (VC).

VC hat keine Benutzeroberfläche auf dem Server, auf dem es installiert ist, sondern stellt nur eine Art Proxy zwischen den VI-Clients und den ESX Servern dar. Die Einstellungen sichert das VC entweder in eine lokale „Microsoft SQL Server Desktop Engine" (MSDE) oder in eine vollwertige Datenbank.

Die Authentifizierung erfolgt über die lokale Benutzerliste oder, sofern verfügbar, das Active Directory. In allen Fällen, in denen in der VI3 mehr als ein ESX notwendig ist, gilt VC als unabdingbare Voraussetzung: etwa für VMotion (Migration), High Availability (Hochverfügbarkeit), Distributed Resource Scheduler und Consolidated Backup. VC bietet nicht nur den Vorteil der gemeinsamen Administrierbarkeit von ESX-Farmen, sondern erlaubt die zentrale Verwaltung von Rollen und Rechten der einzelnen Administratoren, die für unterschiedliche VMs, ESX-Farmen und das VC zuständig sind.

Hinzu kommt der Lizenzserver, der oft auf der gleichen Maschine läuft wie das VC. Da es für alle einmal lizenzierten Optionen eine Spanne von zwei Wochen gibt, in der er nicht erreichbar sein darf und auf ihm keine sicherheitskritischen Daten gespeichert sind, bleibt er in diesem Artikel außen vor.

Eine wichtige Rolle spielt die Farm, eine Gruppe von ESX Servern in einer VI, die eine bestimmte Aufgabe haben oder zu einer Abteilung oder einem Kunden gehören. Innerhalb einer Farm kann es durchaus produktive Systeme wie Test- und Entwicklungsumgebungen geben. In einer VI sind die Server in der Regel an ein Storage Attached Network (SAN) angeschlossen, das über Logical Unit Numbers (LUNs) Speicherbereiche bereitstellt. Die Größe einer Farm schränken drei Faktoren ein: die Zahl der Server, die gleichzeitig auf eine LUN zugreifen, wie viel Rechner dort gespeichert sind und der gewünschten Durchsatz im SAN. Große VI-Umgebungen können über mehrere Farmen verteilt sein.

## Trennung vom Netz der Netze

Alle Komponenten einer VI benötigen ein gemeinsames Verwaltungsnetz, über das die Steuerung und der Datenaustausch stattfinden kann. Um zu verhindern, dass eine VM die Kommunikation stört oder ein Angreifer, der sie übernommen hat, die Komponenten der VI angreift, muss das Verwaltungsnetz von den produktiven Netzen der VMs getrennt sein. Zudem sollte es keine Verbindungen zu anderen internen Netzen im Unternehmen geben. Die Trennung kann physikalisch mit separaten Switches oder virtuell mit einem VLAN geschehen. Das COS sollte nicht die gleiche Netzwerkkarte nutzen wie die VMs. Gleiches gilt gegebenenfalls für VMotion und Speichernetze, die etwa iSCSI nutzen. Welches Level infrage kommt, hängt vom angestrebten Sicherheitsniveau und den zu rechtfertigenden Kosten ab. Datenbankserver und Lizenzserver brauchen nur einen Zugang zum VI-Netz und sollten darauf beschränkt bleiben.

Da die Arbeitsplätze der Administratoren oft im Intranet angeschlossen sind, empfiehlt es sich, VC mit zwei Netzwerkkarten auszustatten: eine für die Kommunikation nach innen mit der VI und eine für den Kontakt nach draußen zu den VI-Clients auf den Arbeitsplätzen der Administratoren. Dort kann das VC an das Active Directory angebunden sein, das die Authentifizierung regelt. Bei besonderen Anforderungen an die Sicherheit kann man das VC vollständig hinter eine Firewall verbannen, die eine Trennwand zwischen dem Intranet und dem produktiven Netz der VI-Komponenten aufbaut.

Nicht aus den Augen verlieren sollte man beim Abschotten, einen Weg für die Übertragung von (VMware-) Images (*vmdk*-Dateien) und den Zugang zum ESX per *ssh* zu schaffen. Außerdem sind die Optionen der Physical-2-Virtual-Migration (P2V) eingeschränkt, wenn die zu migrierende Maschine nicht über den Port 903 mit einem ESX kommunizieren kann. Wie der Zugang aussehen sollte, hängt von der Umgebung ab. Bewährt hat sich der Transport von Dateien per *scp* von den Clients der Administratoren aus, weil es über den SSH-Port des ESX geht, sodass für beide Funktionen nur ein Port für die einzelnen IPs des Intranet offen sein muss.

Per Port Forwarding über SSH sind die erweiterten Funktionen auf Port 903 für eine direkte Systemmigration auf einen ESX Server erreichbar. Wichtig ist es, dass der beim Einrichten des ESX Server angelegte Benutzer „Root“ sich nicht über *ssh* anmelden darf. Jeder Administrator, der das COS nutzen und Migrationen durchführen soll, muss als Benutzer im ESX existieren.

Es gibt drei Anwendergruppen: Nutzer und Administratoren der VMs sowie die Administratoren der VI. Erstere benötigen keinerlei Rechte auf den Komponenten der VI und sollten dazu keinen Zugang haben. Innerhalb der Gruppe der VI-Administratoren kann es wiederum feine Unterschiede geben, je nachdem, welche Person welche Rolle erfüllt und welche Rechte damit verbunden sind. Für alle Farmen, eine Farm, einen ESX oder nur eine VM können Benutzer das Recht erhalten, neue Server aufzunehmen, VMs hinzuzufügen, deren Einstellungen zu ändern, sie zu rebooten oder die Konsole der VM aufzurufen.

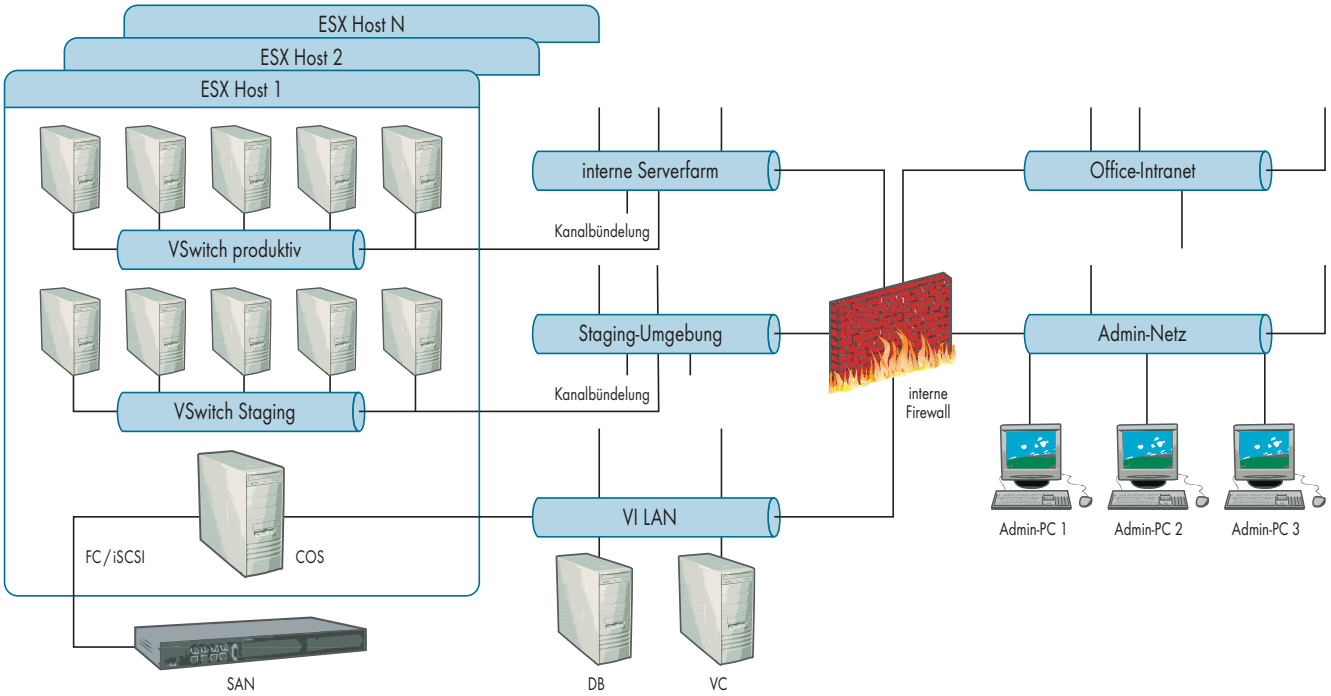
## Einmalige Admin-Aufgabe

Der erste einzurichtende User jedes neuen ESX heißt ROOT. Er hat nur einmal die Aufgabe, den Server in die Verwaltung des VC aufzunehmen. Später gibt es im ESX nur noch die Administratoren mit lokaler Zuständigkeit, zu denen die Live-Migration ohne den Umweg über Dateien oder VC gehören kann, und diejenigen mit Rechten zur Übertragung von Dateien, die Accounts auf dem ESX benötigen. Im VC gibt es ebenfalls einen Superuser, der über alle Rechte verfügt und Rechte vergeben darf. Ohne AD ist es immer der lokale Administrator Account. Empfehlenswert ist es, nicht die Admins der Domänen für die Rolle einzutragen, da sie in der Regel nur Rechte auf den Windows-VM benötigen.

In einer überschaubaren Umgebung existiert üblicherweise eine Gruppe von Administratoren, die – bis auf die Rechtevergabe und die VC-Verwaltung – alle übrigen Freiheiten einschließlich des Zugangs zum COS haben. Für eine weitere Untergliederung ist es sinnvoll, die

### iX-TRACT

- Die Sicherheit der gesamten virtuellen Infrastruktur (VI) von VMware fußt auf der Zuverlässigkeit der Hardwareplattform.
- Entscheidend ist ein Konzept, das eine saubere Trennung des Verwaltungsnetzes von den produktiven Netzen und von der übrigen Infrastruktur im Unternehmen festlegt.
- Einige Komponenten der VI bedürfen besonders sorgfältiger Prüfung: neben den ESX Servern vor allem das Virtual Center und die Konfigurationsdatenbank.
- Virtuelle Maschinen mit unterschiedlichen Sicherheitsanforderungen sollten nicht im selben virtuellen Netz laufen.




**Viele Wege: Für die Sicherheit beim Einsatz von VMwares Infrastructure 3 ist es unabdingbar, die einzelnen Netze voneinander zu trennen, da es sonst zu Übergriffen kommen kann (Abb. 1).**

Gruppe klein zu halten und eine weitere Gruppe an Administratoren einzurichten, die nur VMs hinzufügen und verwalten können, aber keine Rechte haben, die Farmen selbst zu verwalten oder auf das COS zuzugreifen. Das Konzept ermöglicht zudem die Mandantentrennung, bei der ein Anbieter von VI-Lösungen seinen Kunden die vollen Rechte auf ihre VMs gibt, aber gleichzeitig die Kontrolle über die VI behält.

## Härtung der Komponenten

Ein kritischer Punkt taucht bei der Authentifizierung der VI-Komponenten untereinander auf. Beim Einrichten legt die Prozedur selbst signierte Zertifikate an, die der Administrator bei der ersten Nutzung akzeptieren muss. Wer Hand anlegen möchte, kann die Zertifikate durch selbst erstellte und CA-signierte ersetzen, sollte das aber bereits während der Installation erledigen. Leider gilt dies nur für die Server, eine Authentifizierung des Clients durch den Server per Zertifikat ist nicht vorgesehen.

Jede einzelne Komponente braucht eigene Methoden zur Härtung. Beim ESX Server ist nur wenig zu tun, solange niemand die grundlegende Default-Einstellung *security=high* verändert. Sie stellt sicher, dass der Zugang zum ESX Server nur über stark verschlüsselte Protokolle führt und eine lokale Firewall alle ausgehenden wie eingehenden Verbindungen blockiert, außer *ssh*, *https* und der über den VMware-eigenen Administrationsport 902. Auf dem COS des ESX sollte keiner weitere Software installieren, höchstens zur Überwachung des Betriebs durch Agenten darf es Ausnahmen geben. Schutzsoftware wie Virenscanner oder Ähnliches gehört auf die VMs und haben im COS nichts zu suchen. Und obwohl es sich beim Console Operating System um ein abgespecktes Linux handelt, dürfen niemals die Patches von Red Hat zum Einsatz kommen, nur die von VMware herausgegebenen enthalten die Anpassungen für das COS. Mit der jüngst erschienenen Version 3.5 verbessert sich die Lage: der neue Service „VI Update Manager“ für die Verwaltung der Patches bedient jetzt ESX und COS.

Eine denkbare Lücke, über die jemand von einer VM aus den Wirt beeinflussen könnte, öffnen die Logfiles, die VMwares Tools auf der VM und die VMware-Instanz auf dem Wirt ablegen. Es könnte zu einem Überlaufen der Platten im ESX kommen. Man kann sie schließen, indem man das Logging komplett abschaltet oder die Dateien in der Größe einschränkt.

Da das VC oft aus mehr als einem Außennetz erreichbar sein soll, entsteht schnell ein Sicherheitsrisiko. Es gelten die Regeln für die Härtung eines Windows Server an besonders exponierter Stelle, wie sie diverse Best Practice Guides und der IT-Grundschutzkatalog des BSI [e] aufführen. Gleiches, in leicht abgeschwächter Form, gilt für den Datenbankserver. Selbst wenn er nicht aus dem Intranet oder dem Verwaltungsnetz erreichbar sein sollte, gilt er wegen der brisanten Daten als primäres Ziel für Angreifer und braucht einen dementsprechenden Schutz. Nach dem Installieren des VC kann man den DB-User, mit dem das VC auf die Datenbank zugreift, in seinen Rechten stark beschneiden.

Für die Sicherheit der gesamten Umgebung sind die Clients relevant, die als Arbeitsplätze der Administratoren fungieren. Wenn dort ein Angreifer einen Keylogger installieren kann, hebelt das alle anderen Sicherheitsmaßnahmen der VI aus, da er mit den Admin-Rechten auf das VC oder den ESX zugreifen kann. Dem sollte man ausreichend Achtung schenken und sich an die Empfehlungen für die Windows-Clients halten. Letztlich bleiben die VMs, die denselben Schutz wie Root-Server genießen sollten.

## Sicherheit des Massenspeichers

Das Datenvolumen in einer VI ist erheblich, unter anderem, weil der ESX Server es nicht wie seine kleineren

Brüder erlaubt, die virtuellen Festplatten (*vmdk*-Dateien) dynamisch bis zur maximal eingestellten Grenze zu vergrößern, sondern beim Anlegen des Massenspeichers für die VM eine Datei erzeugt, die genauso groß ist, wie sie dort erscheint. Nur für Tests und kleine Installationen kann man deswegen die lokalen Festplatten des ESX für eine VM nutzen, kann dann aber nicht die erweiterten Funktionen der VI wie High Availability, Distributed Resource Scheduler und VMotion nutzen. Es bedarf eines Speichermediums, das allen ESX einer Farm gleichzeitig zur Verfügung steht. VI unterstützt SAN über Fibre Channel (FC) oder seit der Version 3 über iSCSI.

## Per LUN separiert

Der Zugriff ins SAN geht über HBAs (Host Bus Adaptors), die im ESX eingebaut sind. Sofern das SAN es unterstützt, erkennt ESX unterschiedliche Pfade zur gleichen LUN und stellt sie automatisch bereit. Bewährt hat es sich, LUNs mit unterschiedlichen SAN-Architekturen für VMs anzubieten, die voneinander abweichende Sicherheitsanforderungen haben. Nicht jede VM benötigt eine über mehrere Standorte gespiegelte LUN oder eine, die als RAID 5 realisiert ist. So kann man Test-VMs und Entwicklungsumgebungen auf LUNs lagern, die weniger aufwendig sind als diejenigen, die auf Ausfallsicherheit getrimmt sind.

Innerhalb der LUNs richtet das System entweder eine VMFS-Partition ein oder gibt die LUN direkt an die VM per „Raw Device Mapping“ (RDM) weiter. Letzteres erlaubt sogar den Betrieb mancher SAN-Verwaltungssoftware in einer VM, während man gleichzeitig Snapshots für die Daten in der LUN erstellen kann. VMs, deren Cluster-Lösung (etwa Windows Cluster) gemeinsam genutzte LUNs benötigen, sind mit RDM realisierbar.

## Schwachpunkt *mount*

Rechte auf den VMs verwaltet ESX auch über Dateisystemrechte. Wer ein VMFS per *mount* einhängen kann, weil er Zugang zu dessen LUN hat, kann die Kontrolle über eine VM übernehmen, obwohl die im VC eingestellten Regeln das verbieten. In einer VI mit mehreren Farmen dürfen auf jedem Host nur die für ihn bereitgestellten LUNs sichtbar sein. Das gilt auch für ESX Server, die zu keiner Farm gehören. Nur eine genaue Planung und Abstimmung der SAN-Zonen und der im SAN angewendeten Masken kann zu einer sauberen Trennung der einzelnen Systeme führen – unter der Voraussetzung, dass das Sicherheitskonzept des SAN das unterstützt.

Auf ihre virtuellen Netze sollten ausschließlich die VMs zugreifen dürfen. Eine Vermischung mit denen der VI ist nicht empfehlenswert, deswegen sollte niemand beim Installieren Default Port Groups einrichten, da sonst die Gefahr besteht, dass jemand in einer VM das Netzwerk des COS oder der gesamten VI-Komponenten sieht.

Für die VMs stellt der jeweilige ESX einen virtuellen Switch (vSwitch) oder eine physische Netzwerkkarte im Server zur Verfügung. Außerdem kann man einen eingehenden VLAN-Trunk auf die Netzwerkkarten der VMs verteilen. ESX agiert als Switch, der einzelne Ports einem VLAN zuordnet. Für die Sicherheitskonzeption ist relevant, dass VMs mit hohen Anforderungen an die Ausfallsicherheit mehr als eine physikalische Netzwerkkarte nutzen. Das kann über eine direkte Zuordnung per Bridging geschehen. Da ein ESX Server sich erst ab vier VMs rentiert, wäre der Bedarf an Karten im Rechner enorm.

Deshalb schließt man üblicherweise die VMs an einen virtuellen Switch an, der wiederum mit bis zu acht physischen Netzwerkkarten an einem oder mehreren physischen Switches angeschlossen ist. Die Netzwerkkarten arbeiten parallel, wobei jede MAC-Adresse eines VM-Ports nur auf einer physischen Netzwerkkarte aktiv sein kann, damit es nicht zu Fehlfunktionen im Netz kommt. Außerdem ist eine Kanalbündelung möglich.

Man kann im ESX für die „Virtual Machine Network Interface Card“ (VMNIC) den VMs den Wechsel der MAC-Adresse verbieten. Wobei „verbieten“ das falsche Wort ist: Wie bei der Port-Security für Switches nimmt ESX den Port in dem Augenblick vom Netz, in dem sich dort beim Senden die MAC-Adresse ändert. Erst wenn wieder die ursprüngliche Adresse in den Ethernet Frames auftaucht, leitet das System sie an die anderen VMs an derselben VMNIC und an die physikalischen Netzwerkkarten weiter. Darüber hinaus kann der Administrator den Promiscuous Mode, in dem alle empfangenen Pakete auf dem Kabel zu sehen sind, den VMs verwehren.

## Benannte VMNICs helfen

Wichtig, wenn auch nur für VMotion, ist, dass auf allen ESX Servern einer Farm die gleichen VMNIC vorhanden sein müssen, damit die VMs nach und während eines Umzugs ihren Kontakt zu ihrem Netz nicht verlieren. Es empfiehlt sich außerdem, die VMNICs sprechend zu benennen. ESX hilft in der GUI, indem es dort die auf der Karte per Sniffer entdeckten IP-Nummern der angeschlossenen Netze anzeigt, sodass man die VMs den richtigen VMNICs leicht zuordnen kann.

Sicherheit heißt in diesem Kontext nicht nur, die VI vor den VMs zu schützen und Letztere vor Malware, Angreifern und allem, was die Trennung der VMs voneinander und die dort gelagerten Daten verändern könnte, sondern auch für Verfügbarkeit zu sorgen.

Um zu verhindern, dass eine VM alle verfügbaren Ressourcen aufbraucht, kann der Systembetreuer für jede VM eine Ober- und Untergrenze für den Gebrauch der Ressourcen setzen. Obergrenzen für produktive VMs sind nur bedingt sinnvoll, da sie bei kurzfristigen Leistungsspitzen nicht mehr reagieren können. Solche, bei denen es im selben Zeitraum zu hohen Lasten kommen kann, sollten prophylaktisch auf unterschiedlichen ESX laufen. Dabei kann VMwares „Distributed Resource Scheduler“ helfen, da bei einem Lastengpass einer VM die VI darauf reagieren und die virtuelle Maschine auf einen nicht ausgelasteten Servern, verlagern kann.

## Fazit

Bei Beachtung aller Sicherheitsmaßnahmen, einem überwachten Betrieb und schnellen Prozessen zum Beheben von Schwierigkeiten ist VMwares Virtual Infrastructure den Anforderungen der Sicherheit an den Betrieb mit produktiven Anwendungen und sensiblen Daten gewachsen. Jedoch wächst der Grad der Komplexität durch die zusätzliche Software und die damit verbundenen administrativen Aufgaben.

VMware schlägt vor, aus Gründen der Lastverteilung, auf einem ESX produktive VMs mit Test- und Entwicklungsumgebungen gleichzeitig zu betreiben, da die beiden Letztgenannten nur selten Ressourcen verbrauchen und viele Speicherseiten mit iden-

tischem Inhalt erzeugen, der nur einmal pro ESX physikalisch existieren muss. Das führt zu einer besseren Auslastung der gesamten Hardware. Zwar sprechen unter Sicherheitsaspekten derzeit kaum Gründe gegen den Einsatz des ESX, trotzdem will ein solcher Schritt gut überlegt sein und nur für VMs gewählt werden, deren Anforderungen an die Sicherheit nicht zu hoch sind.

Ähnliches gilt für die Vermischung von VMs aus Zonen mit unterschiedlichen Sicherheitsanforderungen in einer durch Firewalls aufgeteilten Umgebung, etwa die unterschiedlichen Segmente einer DMZ. Nach dem derzeitigen Kenntnisstand beeinträchtigt die Virtualisierung die Sicherheit der VMs in einer solchen Architektur gering, erhöht sie sogar unter Umständen, da man Konzepte wie Ausfallsicherheit in der VI mit weniger Aufwand und gleich für mehrere Systeme realisieren kann. Trotzdem bestehen Gefahren, wie sie durch unabsichtliche Fehlkonfigurationen oder Fehler in der Virtualisierungstechnik entstehen können. VMs, deren Sicherheitsklassen weit auseinanderliegen, sollten auf keinen Fall zur selben VI gehören. (rh)

CHRISTOPH PUPPE

ist Sicherheitsberater bei der HiSolutions AG, Berlin.

## Onlinequellen

| | |
|---|---|
| [a] Evaluation Assurance Level | www.commoncriteria.de/index.php?option=com_content&task=view&id=8&Itemid=60 |
| [b] Protection Profiles | www.commoncriteria.de/index.php?option=com_content&task=view&id=9&Itemid=2 |
| [c] Common Criteria | www.commoncriteriaportal.org |
| [d] Verwundbarkeit von VI3 | archives.neohapsis.com/archives/fulldisclosure/2007-09/0356.html |
| [e] Windows Server härten | www.bsi.de/gshb/deutsch/baust/b03108.htm |

## Literatur

[1] Sven Ahnert; Virtualisierung; Transparente Verbindlichkeiten; Stärken und Schwächen von VMwares Infrastructure 3; *iX* 9/2007, S. 70

[2] Stefan Gora; Rootkits; Bittere Pille; Schadsoftware beutet Hardware-Virtualisierung aus; *iX* 4/2007, S. 120

[3] Alexander Geschonneck; Computerforensik; Wiederbelebung; Festplatten-Images mit Live View unter VMware analysieren; *iX* 4/2007, S. 139

[4] Michael Ziegler; Virtualisierung; Desktop zentral; VMwares Konzept der Virtual Desktop Infrastructure; *iX* 8/2006, S. 110

[5] David Ochel; Zertifizierung; Garantiert sicher; Evaluierung von IT-Sicherheit; *iX* 5/2005, S. 132