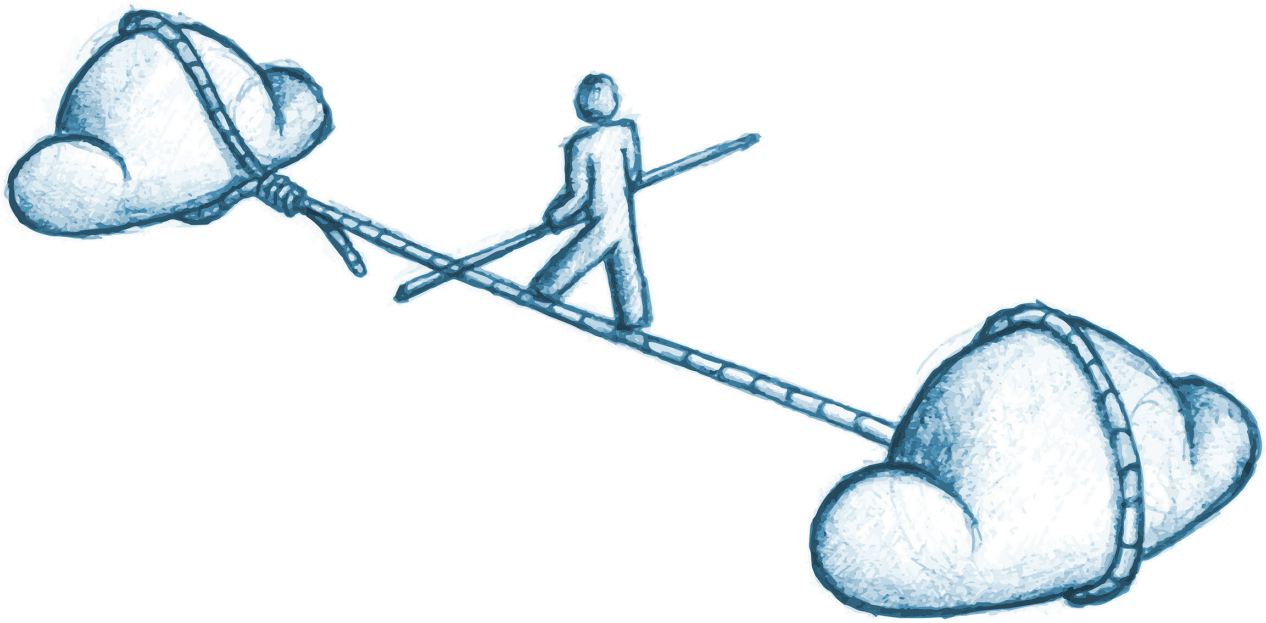
Livre blanc

Bitdefender

Évoluer ou mourir : L'adaptation de la sécurité au monde virtuel

Bitdefender

Table des matières



Bitdefender®

La virtualisation est omniprésente

L'utilisation de la technologie de virtualisation x86 a régulièrement progressé depuis le début des années 2000. En 2011, la société Veeam a suivi l'adoption de la virtualisation dans les entreprises et a constaté que **39,4% des serveurs d'entreprise étaient des systèmes virtuels,** un chiffre qui est probablement encore en hausse. De plus, **91,9% des entreprises ont opté pour une technologie de virtualisation sous une forme ou une autre,** ce qui indique son adoption massive et générale.[1] Selon l'étude réalisée par Cisco en 2013, les principales motivations de son adoption sont la plus grande efficacité et les économies engendrées. Son plus grand point fort : une **meilleure évolutivité du système,** en particulier dans le cas des nouveaux déploiements.[2]

La virtualisation ne présente toutefois pas que des avantages. La mise en place de cette technologie peut facilement se traduire par des incompatibilités avec la technologie de sécurité installée, des problèmes de gestion et de cryptage des fichiers et des pertes de performances liées à l'utilisation des solutions antimalwares traditionnelles, entre autres.

L'évaluation de l'ampleur du problème selon le PCI Standards Council (2011)

En juin 2011, le Conseil des normes de sécurité PCI (Payment Card Industry) a publié un supplément informatif attendu depuis très longtemps, qui complète la norme de sécurité des données (DSS) et qui se nomme PCI DSS Virtualization Guidelines. Ce guide collaboratif, réalisé par un groupe d'experts en sécurité et en conformité, regroupe des conseils à l'intention des équipes informatiques, en particulier des experts, pour procéder à l'évaluation des infrastructures virtualisées qui rentrent dans le champ d'application des obligations de mise en conformité des cartes de paiements. Deux parties essentielles de ce document se démarquent : la première présente les risques de la virtualisation ; la seconde formule des recommandations de contrôle. Elles sont toutes les deux pertinentes pour atteindre l'objectif visé, la protection des données dans les environnements virtualisés. Parmi les risques présentés dans ce document du PCI, on peut citer[3] :

- **Les vulnérabilités présentes au sein des environnements physiques s'appliquent également aux environnements virtuels :** "les menaces des environnements physiques s'appliquent également aux environnements virtuels ; même les partitions logiques configurées de la façon la plus sûre nécessiteront des contrôles physiques adaptés afin de protéger le hardware".

- **Une complexité accrue des systèmes et réseaux virtualisés :** l'ajout de nouvelles couches technologiques telles que les appliances et réseaux virtuels, ainsi que l'hyperviseur lui-même, génère des problèmes potentiels de configuration. Ces derniers, parfois associés à des vulnérabilités de virtualisation, peuvent créer d'importants facteurs de risque.

- **L'association de VM de différents niveaux de confiance :** selon les conseils du Conseil des normes de sécurité PCI, associer différents niveaux de classification des données sur un hyperviseur unique pourrait conduire à une perte ou une divulgation de données, ce qui pourrait également s'appliquer logiquement au stockage des images de VM.

- **L'absence de séparation des tâches :** ne pas définir les rôles, ni attribuer les privilèges correctement, pourrait entraîner l'attribution d'un accès privilégié à bien plus que la console de gestion de la virtualisation elle-même.

- **Les machines virtuelles inactives :** "les VM qui ne sont pas actives (inactives ou plus utilisées) peuvent encore contenir des données sensibles telles que des informations d'authentification, des clés de cryptage ou des informations de configuration critiques."

- **Les images et les snapshots de VM :** "… si des images ne sont pas protégées contre les modifications, un attaquant peut y accéder et insérer des vulnérabilités ou du code malveillant dans l'image. L'image corrompue pourrait ensuite être déployée dans l'environnement, provoquant la corruption rapide de multiples hôtes."

Le Conseil des normes de sécurité PCI recommande également de suivre les mesures s'appliquant spécifiquement à la protection des données suivantes :

- **Évaluer les risques liés aux technologies virtuelles :** évaluer les risques de tous les composants et processus de virtualisation, comme pour toute autre technologie.

1 - http://www.veeam.com/news/veeam-launches-v-index-to-measure-virtualization-penetration-rate.html
2 - http://ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=461862&SWTHEMEID=12949
3 - https://www.pcisecuritystandards.org/documents/Rth87Wp/Virtualization_InfoSupp_v2.pdf

- **Limiter l'accès physique :** veiller à ce que l'accès physique aux VM et plates-formes de virtualisation soit limité et surveillé de près.
- **Mettre en place une défense en profondeur :** des contrôles de sécurité devraient être envisagés et éventuellement appliqués à tous les niveaux technologiques dont les systèmes physiques, l'hyperviseur, les plates-formes des hôtes et de VM, les applications et le stockage.
- **Mettre en place le moins de privilèges possible et séparer les tâches**
- **Sécuriser les machines virtuelles et les autres composants :** la sécurisation et le verrouillage devraient inclure les interfaces réseau virtuelles et les zones de stockage ; l'intégrité de toutes les opérations de gestion des clés de cryptage devrait être vérifiée.

La publication de ces conseils prouve à quel point la virtualisation était essentielle et courante dès 2011. Notons qu'il s'agit de l'unique guide de conformité officiel sur la sécurité de la virtualisation publié à ce jour !

Les nombreux défis liés à la sécurité

Ces dernières années, les équipes de sécurité ont rencontré de nombreux défis. Les sections suivantes présentent certains de ces défis et la façon dont ils ont été résolus.

L'entrave à la bonne gestion des inventaires liée à la prolifération des VMs

Les équipes de sécurité sont aux prises avec des datacenters qui ne sont pas des systèmes physiques mais de simples ensembles de fichiers hébergés par des hyperviseurs et stockés dans un réseau de stockage (SAN) ou un autre environnement de stockage. Cela conduit au premier problème, la gestion des inventaires.

Dans le projet SANS 20 Critical Controls, l'absence d'inventaire des équipements et des logiciels fait systématiquement partie des deux principaux problèmes figurant dans la liste[4]. La virtualisation permet une création et une propagation bien plus rapides d'applications et de systèmes opérationnels puisqu'elle ne nécessite que la création d'un autre ensemble de fichiers, et aucun matériel supplémentaire. Un administrateur peut créer une machine virtuelle en quelques secondes et la faire fonctionner dans un environnement de production en quelques minutes. Cela peut facilement conduire à un grand nombre de systèmes sur lesquels pas ou peu de contrôles du cycle de vie sont appliqués.

L'archivage et la destruction des données constituent également des étapes essentielles du cycle de vie des données. Dans les environnements virtualisés, cela implique de surveiller l'ensemble des machines virtuelles et des données auxquelles on accède et que l'on conserve pour une utilisation dans ces environnements virtualisés. Les machines virtuelles conservées entièrement sur des bandes de sauvegarde ou sur d'autres supports ne peuvent pas être stockées en toute sécurité si le support de sauvegarde n'est pas crypté. Une autre possibilité consiste à mettre hors service des machines virtuelles entières et à les retirer de la circulation. Sans une bonne gestion de l'environnement virtualisé et de ses composants, il est probable que **des données confidentielles demeurent présentes sur les disques des VM ou dans des fichiers liés à la mémoire** et que certaines d'entre elles soient oubliées si aucune mesure de précaution adaptée n'est mise en place. En d'autres termes, ce n'est pas aussi simple que de détruire un serveur physique.

Une machine virtuelle étant simplement un ensemble de fichiers, elle constitue une cible de choix pour les attaquants. Voler une machine est aussi simple qu'effectuer un copier/coller de fichiers.

Par exemple, dans les environnements VMware, une machine virtuelle (appelée ici "VM") contient un certain nombre de fichiers spécifiques :

- VM.vmx : le fichier de configuration de la VM
- VM.vmdk : le fichier de configuration du disque virtuel
- VM-flat.vmdk : le disque dur de la VM
- VM.nvram : le fichier BIOS de la VM

4 - http://www.sans.org/critical-security-controls

• VM*.log : le fichier journal de la VM

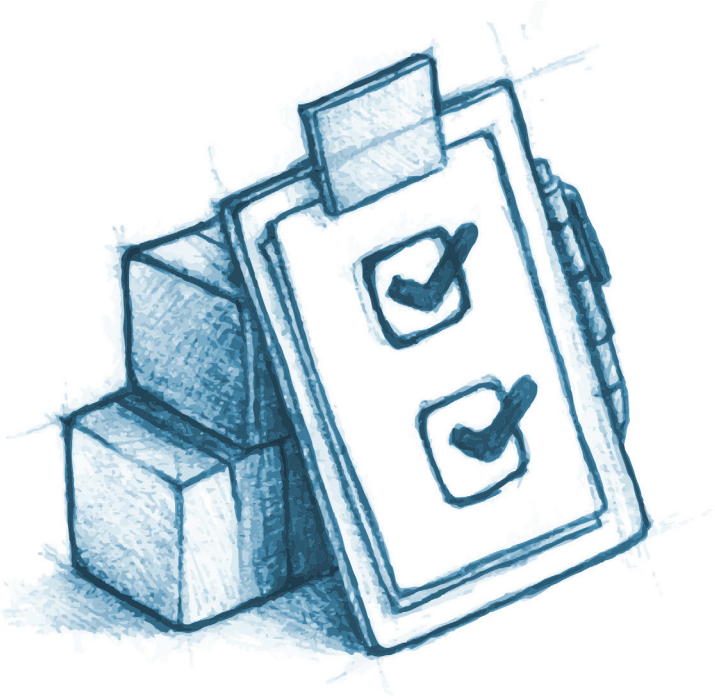
• VM.vswp : le fichier d'échange de la VM

• VM.vmsn/vmsd : les métadonnées du snapshot de la VM

• VM0000001-delta.vmdk : le fichier d'écriture du snapshot en temps réel

• VM-***.vmss : les données de la mémoire de VM suspendues

Tous ces fichiers n'existent pas simultanément ; ils dépendent de l'état des VM. Ils sont tous importants et **certains, s'ils ne sont pas protégés, peuvent contenir des données sensibles.** Par exemple, le fichier d'échange des VM (vswp) et celui de suspension (vmss) peuvent contenir des mots de passe, des clés de chiffrement ou des données d'applications sensibles. Un attaquant pourrait accéder à ces données et les dérober lorsque ces fichiers sont stockés. Du point de vue de la configuration, le fichier .vmx est le plus important et un certain nombre de paramètres spécifiques, dans ce fichier, peuvent contribuer à protéger la VM, avec des contrôles allant des paramètres de journalisation à l'interaction avec le système de l'hyperviseur. On retrouve ces types de fichier dans tous les principaux environnements de virtualisation dont Citrix, Microsoft et KVM, entre autres.



La plupart des entreprises sont actuellement aux prises avec la **gestion des inventaires** de l'ensemble de leurs biens, qui vont au-delà des machines virtuelles et des applications. Cependant, de nouveaux outils d'éditeurs leaders en virtualisation (VMware, Microsoft, Citrix etc.) et des solutions tierces axées sur la gestion du cycle de vie des VM peuvent s'avérer utiles dans une certaine mesure. La plupart des situations de prolifération des VM sont dues à de mauvais processus et au manque d'attention portée aux politiques de sécurité et de cycle de vie. Par exemple, lorsqu'un développeur a besoin d'un nouveau système pour effectuer des tests, un système de surveillance et de restrictions devrait limiter la durée pendant laquelle la VM peut fonctionner avant d'arriver à expiration. Automatiser la création des VM constitue en soit la moitié du travail, cependant ceci augmente le ratio entre le cycle de vie des VM et la gestion des composants.

La classification et le cryptage des VM mobiles

Alors que les entreprises cherchent à améliorer leurs infrastructures de virtualisation en passant au cloud privé ou hybride, le problème de la sécurité des machines virtuelles mobiles dans le cloud doit être réglé. Plusieurs aspects essentiels sont à prendre en compte parmi lesquels :

- **Les données en texte clair en transit :** utiliser vMotion et d'autres techniques similaires de migration des VM met en danger la mémoire des VM et peut permettre à toute personne surveillant le réseau, par lequel ces données transitent, d'accéder aux données d'applications et de fichiers.

- **L'environnement multi-tenant :** des VM de différents niveaux de classification hébergées sur le même hyperviseur peuvent entraîner la divulgation de données sensibles si la classification des systèmes n'est pas effectuée lors de la migration des données et des VM. De nombreuses entreprises réalisent mal la classification des données et des environnements cloud complexes peuvent facilement avoir plusieurs opérations de migrations de VM simultanément. Par exemple, une VM hébergeant des applications de traitement de données bancaires pourrait être migrée vers un hyperviseur hébergeant des systèmes bien moins sensibles, ouvrant potentiellement une nouvelle voie à la divulgation de données.
- **La sécurité des données "at rest" (stockées) :** les données "at rest" correspondent généralement aux données écrites sur le disque. Puisqu'une machine virtuelle est simplement un ensemble de fichiers, toute la VM peut, et souvent devrait, être cryptée sur le disque lorsque cela est possible. L'image de la VM en cours d'exécution n'est pas le seul endroit pouvant contenir des données sensibles. Les snapshots, images de sauvegarde et images de mémoire de VM suspendues peuvent également contenir des informations qui devraient être protégées.

Pour régler ces problèmes de sécurité, nombreux sont ceux qui recherchent de nouveaux mécanismes de sécurité permettant d'appliquer les politiques lorsque les machines virtuelles sont déplacées.

Pour être efficaces, des politiques de sécurité doivent être créées et appliquées au sein d'une solution de virtualisation et être reconnues par chaque hyperviseur hébergeant la machine virtuelle lorsque celle-ci est déplacée.

Les services de cryptage impliquent généralement des clés. Maintenir les clés confidentielles hors de portée des attaquants ou des administrateurs des fournisseurs de clouds est une dimension supplémentaire à prendre en compte. De nombreuses options sont disponibles afin de faciliter la gestion de la sécurité et le cryptage dans les clouds. Les nouvelles solutions de HyTrust, CipherCloud, CloudLink, SafeNet, et même des services de gestion de clés de Porticor et d'autres prestataires, peuvent contribuer à simplifier le cryptage à la fois dans le datacenter et lors de la migration vers des fournisseurs de clouds publics.

Amazon est un exemple de fournisseur de cloud se tournant vers le **cryptage géré par les clients.** Il permet à ses clients de gérer leurs propres clés pour les volumes de stockage montés dans les instances EC2, ou sur Amazon S3 dédiés et fournissent même une plate-forme dédiée au stockage des clés cryptographiques.

La plupart des fournisseurs de virtualisation (et des fournisseurs de clouds) comme VMware et Microsoft recommandent désormais d'utiliser des outils de chiffrement dans les VM afin de protéger les données dans les environnements cloud publics et privés. L'une des principales préoccupations des équipes opérationnelles quant à cette approche est l'impact potentiel que peuvent avoir les processus de chiffrement et de déchiffrement sur les opérations de virtualisation.

L'adaptation de longue date des malwares aux environnements virtualisés

Alors que les malwares n'hésitaient pas, au début, à infecter les VM (Windows est Windows quel que soit l'environnement), les choses ont quelque peu évolué. L'une des tendances les plus inquiétantes depuis 2006 est l'apparition de malwares adaptés spécifiquement aux VM. Ces types de bots, virus, rootkits et autres sont capables d'utiliser un certain nombre de techniques, simples ou élaborées, afin de déterminer s'ils sont exécutés sur un hôte physique ou virtuel. Lorsque le malware détecte qu'il se trouve dans un environnement virtuel, il peut refuser de s'exécuter ou se comporter autrement que sur un hôte physique.

Imaginez un malware ciblant les systèmes d'exploitation d'utilisateurs finaux. La plupart des utilisateurs finaux n'exécutent pas leurs systèmes dans des environnements virtuels. En revanche, la plupart des éditeurs de sécurité ont des systèmes d'exploitation pour utilisateurs finaux dans des environnements virtualisés pour la même raison que celle pour laquelle toute entreprise opte pour la virtualisation.

En effectuant des actions inoffensives ou en demeurant inactifs, les auteurs de malwares espèrent échapper à l'analyse automatisée offert par la virtualisation et aux honeypots (systèmes déployés afin de paraître normaux mais qui sont en fait étroitement surveillés pour mieux comprendre les techniques d'infection).

Bitdefender

L'impact des antimalwares sur les performances

En plus des nouvelles **menaces ciblant spécifiquement les environnements virtualisés,** la simple mise en place d'un antimalware pose de plus en plus de problèmes dans ces environnements.

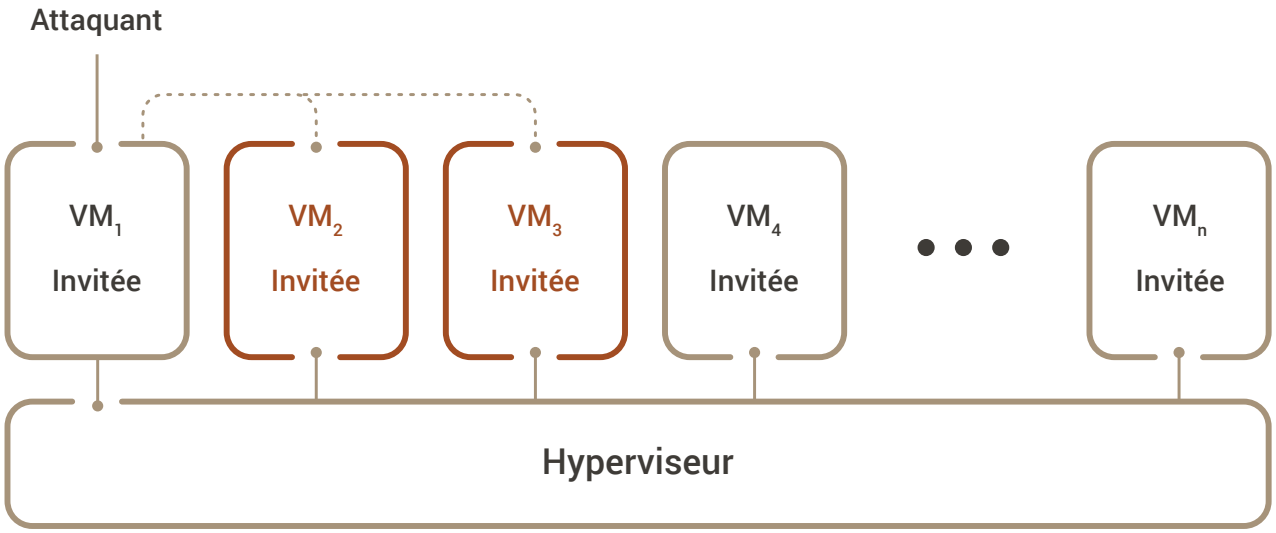
Les administrateurs sont réticents à installer des outils antimalwares traditionnels dans des environnements informatiques virtualisés par crainte que les ressources nécessaires ne soient trop importantes. Avec un agent antimalware complet, une machine virtuelle consomme davantage de processeur et de mémoire que prévu. Cet effet est multiplié en fonction du nombre de machines virtuelles s'exécutant sur un hôte. Alors que la virtualisation centralise et déduplique une grande partie des ressources utilisées par les machines virtuelles via le modèle des ressources partagées, les antimalwares traditionnels dupliquent la consommation des ressources dans chaque machine virtuelle sans exceptions.

Cela devient particulièrement important **lorsqu'on adopte des clouds hybrides et publics.** Utiliser un agent de sécurité plus léger et souple peut éviter d'importants dépassements de coûts dus à l'utilisation des ressources et l'inadéquation des licences proposées dans l'environnement d'un fournisseur de cloud. Les entreprises devraient chercher à comprendre si les outils de sécurité peuvent fonctionner efficacement dans les environnements cloud publics.

La surveillance des intrusions et la détection des menaces ciblant les VMs, le manque de visibilité et de contrôle

De nombreux nouveaux types de menaces existent dans les environnements virtualisés. Certains sont d'ordre opérationnel et concernent la consommation de ressources et leur disponibilité ou la divulgation de données sensibles transmises sans cryptage.

Un autre problème de sécurité particulièrement évoqué avec les plates-formes de virtualisation est la notion de "VM Escape" (sortie de machine virtuelle), lorsque du code s'exécutant dans une VM est capable de "s'échapper" vers l'hôte de l'hyperviseur sous-jacent.



C'est le pire cauchemar des professionnels de la sécurité : des zones de confiance sont violées, des contrôles d'accès sont contournés, des privilèges s'avèrent probablement inutiles et la confidentialité et l'intégrité des hôtes des hyperviseurs deviennent douteuses.

La plupart des professionnels de la sécurité considèrent actuellement qu'une "VM escape" peut se produire. Depuis 2006, plusieurs outils publiés et présentés lors de conférences permettent le transfert de données entre des machines virtuelles, de même qu'entre des machines virtuelles et l'hôte sous-jacent.

En **décembre 2005,** Tim Shelton a signalé un dépassement de la mémoire tampon (Buffer overflow) dans la capacité de mise en réseau NAT de VMware Workstation, Player, ACE, et GSX Server. Cette vulnérabilité permettait à un attaquant d'envoyer des commandes FTP malformées de l'invité vers l'hôte, via la mise en réseau NAT, entraînant l'exécution de code dans l'hôte sous-jacent.

La plupart des failles de "VM escape" signalées à ce jour sont liées à une forme d'attaque de "directory traversal" (traversée de répertoire). La première d'entre elles a été signalée en **avril 2007** par iDefense, qui décrivait un problème avec la fonctionnalité Dossiers Partagés dans VMware Workstation. En raison d'un problème avec la manière dont Workstation interprétait les noms de fichier, un utilisateur malintentionné pouvait écrire des fichiers depuis un invité vers l'hôte sous-jacent avec les privilèges de l'utilisateur exécutant VMware Workstation sur l'hôte. Intelguardians (devenu InGuardians) s'est appuyé sur cette étude pour sa présentation sur les problèmes de sécurité des VM au cours de la conférence SANSFIRE qui s'est tenue en 2007 à Washington DC.

En **février 2008,** les chercheurs de Core Security (la société qui crée les outils de tests d'intrusion Core IMPACT) ont signalé une faille dans certaines versions de VMware Workstation, ACE et Player permettant à un attaquant d'exploiter localement ou à distance la fonctionnalité des Dossiers Partagés et d'écrire ou de lire dans toute zone de l'OS de l'hôte sous-jacent.

Ces failles ne sont pas considérées comme étant de véritables "VM escape" car le code doit s'exécuter à la fois sur la VM et l'hôte pour que les outils fonctionnent correctement. Une véritable "VM escape" ne dépend pas du code s'exécutant sur l'hôte, ce qui permet à une attaque exclusivement orientée invité de s'échapper de la VM et de commencer à s'exécuter sur l'hôte. De véritables "sorties" semblent toutefois se produire de nos jours. La société VUPEN est parvenue à développer un exploit permettant deux scénarios de "sortie" fortement médiatisés, l'un pour la faille Xen CVE-2012-0217[5] et l'autre **mi-2014** pour VirtualBox[6]. Ils permettent un accès avec les plus hauts privilèges aux ressources de l'hôte à partir d'une VM s'exécutant dans l'environnement tant que l'attaquant dispose de l'accès utilisateur/processus à la VM.

Dans un article publié en **novembre 2012,** des chercheurs ont prouvé qu'il était possible d'effectuer une attaque "latérale" à l'encontre de VM fonctionnant avec la même plate-forme d'hyperviseur[7]. Lors de l'attaque, une VM submerge le cache de l'équipement local, ce qui oblige la VM ciblée à devoir écraser certaines de ces données avec les siennes. En fonction des données écrites et de la façon dont elles sont écrites, les attaquants peuvent percevoir certaines données concernant la VM ciblée, dont des clés de chiffrement utilisées pour l'isolation et d'autres fonctionnalités de chiffrement.

L'accès aux VM devrait être attentivement contrôlé, à la fois par l'attribution de rôles et de privilèges pour l'accès et l'interaction ainsi que par la surveillance et l'audit de l'infrastructure de stockage sur laquelle les VM se trouvent. Cela dépendra du type de stockage dont vous disposez ainsi que des capacités de monitoring d'outils tels que les plates-formes SIEM (Security Information and Event Management) et de gestion des journaux. Les entreprises devraient prêter attention aux types d'activités et aux actions suivantes :

- Quels utilisateurs accèdent aux fichiers de machines virtuelles ?
- D'où proviennent ces utilisateurs ?
- Quel type d'accès est utilisé, allant de l'accès à la console de gestion de la virtualisation à l'accès au partage de fichiers à distance à l'aide des identifiants du domaine ?
- Quand l'accès et/ou les actions ont eu lieu ?

Les outils de sécurité réseau traditionnels ne disposent généralement pas des bons outils pour la virtualisation et sont incapables de surveiller les communications entre VM ou entre les VM et les hôtes. Beaucoup s'inquiètent du fait que le trafic entre VM pourrait transmettre des attaques et des malwares avec peu ou pas de possibilité de les détecter au sein de l'infrastructure virtuelle. Cela était effectivement le cas pendant un certain temps et le réseau virtuel était considéré comme une sorte de "boîte noire" opaque.

Heureusement, de nouveaux outils sont apparus sur le marché et la détection d'intrusions peut être effectuée à l'aide de plusieurs méthodes courantes aujourd'hui. VMware a lancé l'API VMsafe (rebaptisée NSX) fournissant des fonctions permettant aux vendeurs de solutions de gestion de la sécurité de proposer des produits surveillant le trafic sans déployer d'agents partout. De plus, l'introduction de ports SPAN dans les commutateurs virtuels distribués (Virtual Distributed Switches) a rendu possible la virtualisation et l'utilisation en l'état de solutions IDS et IPS traditionnelles, avec des commutateurs virtuels de Microsoft, VMware et Open vSwitch utilisés par Citrix. Le support de Netflow sur les commutateurs virtuels a également grandement amélioré la visibilité du trafic réseau au sein de l'infrastructure virtuelle, permettant aux équipes de sécurité et de réseau de concevoir plus efficacement des références comportementales du trafic au sein d'un environnement virtuel.

5 - http://www.vupen.com/blog/20120904.Advanced_Exploitation_of_Xen_Sysret_VM_Escape_CVE-2012-0217.php
6 - http://www.vupen.com/blog/20140725.Advanced_Exploitation_VirtualBox_VM_Escape.php
7 - http://phys.org/news/2012-11-vm-rude-awakening-virtualization.html

Comment nos politiques, nos processus et nos technologies devront changer pour s'adapter

La virtualisation et les clouds privés concernent l'ensemble de l'infrastructure informatique : l'OS des serveurs traditionnels, les applications et les bases de données, le stockage, la mise en réseau ainsi que le poste de travail. On ne peut changer la façon dont ces composants interagissent sans modifier les politiques qui régissent ces relations ainsi que les processus utilisés pour gérer l'environnement.

L'incapacité à suivre les modifications, approuvées ou non, au fil du temps est amplifiée au sein d'une infrastructure virtuelle. Alors que des machines virtuelles sont constamment provisionnées et déplacées dans l'infrastructure, elles commencent à se diversifier, notamment après des patches et des interactions avec les utilisateurs finaux. Au fil du temps, la machine virtuelle qui était au départ provisionnée à partir d'une version sécurisée approuvée, passe à un état autre que celui du modèle initial. Cette modification présente un risque pour l'entreprise en matière de sécurité et il devient également plus difficile de diagnostiquer les défaillances du système. Si les problèmes de contrôle des modifications sont considérés conjointement avec le prochain défi, la traçabilité, de nombreuses entreprises auront des difficultés à prouver leur connaissance et leur gestion du suivi des modifications aux auditeurs.

Les entreprises sont généralement incapables d'assurer le suivi de la traçabilité des machines virtuelles alors qu'elles passent par différentes étapes : développement, test et production. Idéalement, le service informatique devrait être en mesure de mettre en place un workflow et des processus suivant chaque VM et prouvant que les VM approuvées à une étape conservent leur intégrité à l'étape suivante. Lorsque les entreprises ne fournissent pas de gestion du cycle de vie, il existe un risque de modifications non approuvées ou, pire encore, d'intégration de données de test et de mécanismes tels que les journaux de débogage et les comptes par défaut dans la version de production de la VM.

Un autre aspect oublié de la sécurité d'une infrastructure de virtualisation est **l'isolement et le contrôle d'accès liés au réseau de gestion** connectant les administrateurs aux serveurs d'administration et les serveurs d'administration aux plates-formes d'hyperviseur. Ce réseau de gestion doit être isolé, dans la mesure du possible (ce qui constitue probablement un changement significatif dans l'architecture et la gestion du réseau). Créer un réseau de gestion isolé avec soin aura un impact important sur les processus que les utilisateurs utilisent quotidiennement pour accéder et contrôler l'environnement. Ce modèle peut également offrir la possibilité de mettre en place davantage de "goulets d'étranglement" dans le réseau avec des contrôles d'accès et un audit en place.

La séparation des tâches est un autre principe de sécurité essentiel à mettre en place pour une infrastructure virtualisée. Dans de nombreuses entreprises, la virtualisation est gérée par les administrateurs Windows ou d'autres systèmes déjà présents. Bien que cela puisse être pratique, gérer et administrer un environnement de virtualisation nécessite de tenir compte de nombreux éléments et devrait idéalement être confié à des équipes adaptées.

La plupart des plates-formes de virtualisation rendent possible **l'attribution de privilèges et la création de rôles suffisamment** précis. De nombreuses équipes d'administration utiliseront un rôle Administrateur intégré (ou son équivalent) et attribueront à la plupart des utilisateurs des rôles leur permettant d'accéder aux machines virtuelles (VM) dans des situations spécifiques. De nombreux privilèges peuvent être affectés, y compris un accès explicite aux zones de stockage définies hébergeant des fichiers de machine virtuelle, ce qui peut contribuer à contrôler l'accès non autorisé aux données. Une planification adaptée, qui constitue souvent un effort considérable, est essentielle pour garantir que les rôles utilisateurs et les privilèges d'accès aux données sont adaptés à l'entreprise.

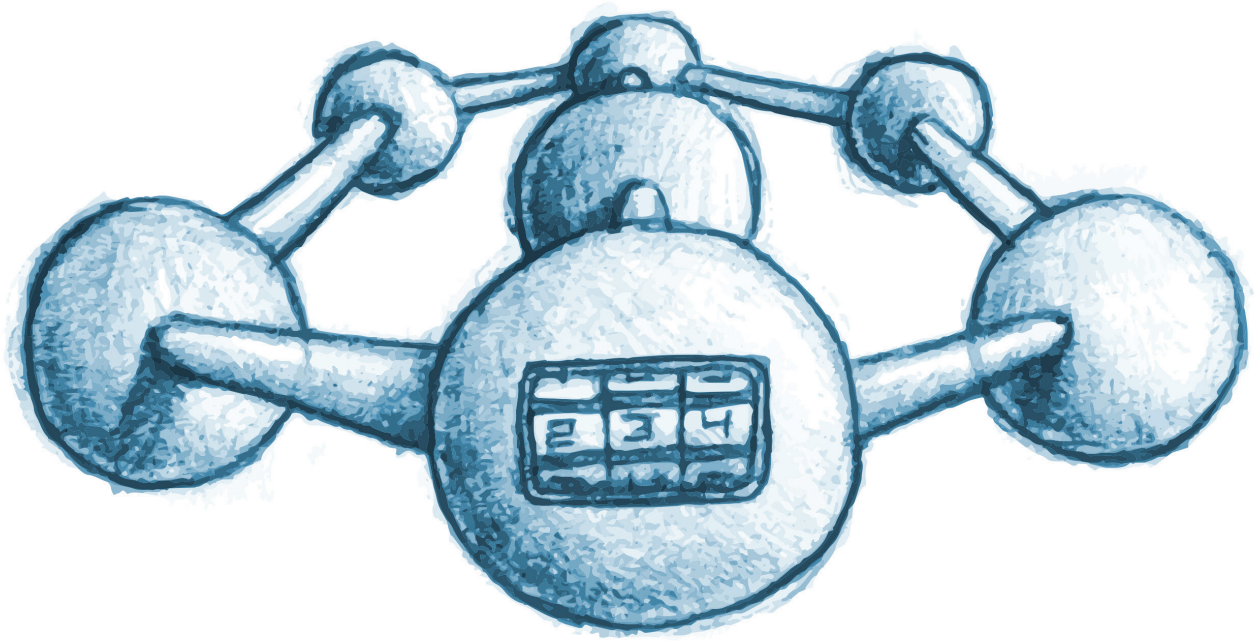
La non-séparation des tâches est souvent associée à une utilisation excessive des privilèges. Les administrateurs de la virtualisation disposent souvent de droits complets sur l'ensemble des objets et des composants de l'environnement, ce qui pourrait facilement avoir des effets dévastateurs si un administrateur de la virtualisation devenait une menace interne légitime (bénigne ou malveillante). Pour gérer correctement les menaces internes et la mauvaise utilisation des systèmes et des données dans les environnements virtuels, les entreprises devraient :

- **Définir des rôles et privilèges relatifs à la virtualisation correspondant aux types d'activités d'opérations informatiques qu'elles aimeraient que l'on réalise dans un environnement physique.** Les membres de l'équipe chargée du stockage devraient être autorisés à gérer le stockage, ceux de l'équipe s'occupant du réseau devraient pouvoir gérer les composants du réseau virtuel, etc. Les membres de l'équipe responsable de la virtualisation devraient être autorisés à configurer et gérer uniquement les composants de la virtualisation (hyperviseurs, outils de sauvegarde et de redondance et pools de ressources dans les clusters), en fonction des besoins. Une autre option est l'utilisation d'outils de PUM (Privileged User Management, gestion des utilisateurs privilégiés) afin d'aider à contrôler les droits d'accès par utilisateurs privilégiés.

- **Appliquer un contrôle d'accès et d'authentification puissants.** Si un réseau de gestion séparé a été mis en place, exigez que tous les accès aux systèmes et outils de gestion proviennent d'une passerelle ou "jump box". Certaines entreprises utilisent également des outils de génération de mots de passe et des mécanismes de jetons d'accès (parfois appelés "password vaults") pour fournir des mots de passe aléatoires à court terme. Cela peut contribuer à verrouiller les demandes d'authentification et fournir également une piste d'audit solide pour le suivi réalisé par les équipes de sécurité.

- **Désactiver l'accès local à la fois aux hyperviseurs et aux machines virtuelles.** Exigez à la place, l'utilisation d'un environnement de services d'annuaire tel qu'un LDAP ou Active Directory pour contrôler de façon centralisée les utilisateurs, les groupes et les droits d'accès aux systèmes lorsque cela est possible.

Enfin, ne partez pas du principe que cela n'arrive qu'aux autres. En juillet 2010, Jason Cornish, employé du service informatique de l'entreprise pharmaceutique Shionogi a supprimé 88 systèmes virtuels en accédant illégalement à un client VMware vSphere masqué qu'il avait installé avant de quitter l'entreprise. Il a été arrêté mais après avoir causé environ 800 000$ de dommages.[8]



Les axes fondamentaux de la sécurité de la virtualisation

Il existe de nombreux types de problèmes de sécurité différents dans les environnements virtualisés, centrés principalement sur les machines virtuelles et leur sécurité globale. Pour résumer, voici quelques-uns des domaines clés sur lesquels se concentrer et le point de vue de l'auteur de ce livre blanc, consultant auprès de grandes entreprises depuis de nombreuses années :

- **La gestion des inventaires demeure un problème majeur.** La prolifération des machines virtuelles est encore difficile à réfréner. D'après notre expérience, au moins 75% des grandes entreprises dans lesquelles une technologie de virtualisation est présente ne disposent pas d'un inventaire précis des machines virtuelles de leur environnement.

- **Le cryptage des environnements virtualisés, allant de la gestion des certificats aux fichiers cryptés de machines virtuelles est encore difficile à mettre en place.** La plupart des entreprises utilisent encore des outils de cryptage et des systèmes de gestion des clés traditionnels qui ne fonctionnent pas toujours correctement sur les machines virtuelles, notamment lors de leur utilisation dans des environnements cloud publics.

8 - http://www.darkreading.com/vulnerabilities-and-threats/virtualization-security-your-biggest-risk-is-disgruntled-insider/d/d-id/1099988?

Bitdefender®

Évoluer ou mourir : L'adaptation de la sécurité au monde virtuel

- **La sécurité basée sur l'OS, notamment les outils antimalwares,** peut paralyser les environnements virtualisés. 90% des entreprises utilisent encore des agents antivirus traditionnels au sein de leurs environnements virtuels, ce qui peut consommer d'importantes quantités de ressources. Des outils plus récents sont capables de limiter la consommation des ressources et il est donc temps pour les entreprises de reconsidérer la façon dont elles protègent les machines virtuelles contre les malwares et les autres menaces.

- **Le monitoring au sein d'un environnement virtuel constitue encore un défi.** La moitié des entreprises ayant recours à une technologie de virtualisation ne journalise pas correctement les événements dans l'hyperviseur (ou d'autres composants) et dans de nombreux cas la surveillance de ce type de réseau n'est pas comparable avec celle opérée pour la détection des intrusions et la surveillance du réseau physique traditionnel.

- **Actuellement, 50 à 75% des entreprises n'affectent pas de rôles dans leurs environnements virtuels et cloud afin de correctement mettre en place une séparation des tâches.** La grande majorité d'entre elles utilise toujours des rôles "administrateurs" génériques avec bien trop de privilèges et ne consacre pas assez de temps à la création de rôles supplémentaires réduisant les privilèges et les permissions. Un administrateur de la virtualisation peut effectuer des actes malveillants dans un environnement virtuel si les droits de gestion du réseau, les méthodes de contrôle des accès, d'authentification et d'audit ne sont pas strictes et si l'attribution des privilèges ne sont pas correctement segmentés.

L'utilisation de la technologie de la virtualisation continue à progresser, de même que le **besoin en mesures de sécurité adaptées,** gérées par les **équipes de sécurité et d'exploitation.** Les risques présentés dans le supplément d'information de 2011 du Conseil des normes de sécurité PCI demeurent d'actualité et le seront probablement tout autant dans un avenir proche. La bonne nouvelle c'est que nous disposons des outils et des connaissances pour commencer à améliorer la sécurité dans les environnements virtualisés et que l'état de la sécurité des environnements virtualisés continuera à s'améliorer avec le temps.

Bitdefender propose une technologie de sécurité dans plus de 100 pays via un réseau de pointe d'alliances, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.

PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender.

Bitdefender®

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.