ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

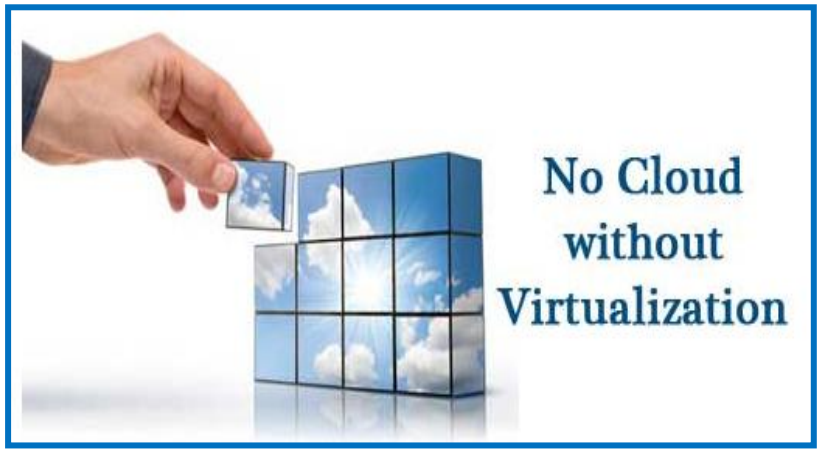
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων»

Κατεύθυνση: «Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διπλωματική Εργασία

Examination of cloud systems' security from virtualization perspective



Μεταπτυχιακός Φοιτητής:

Κολόμβος Ιωάννης ΜΤΕ 1517

Πειραιάς, Μάρτιος 2017

Επιβλέπων:

Λαμπρινουδάκης Κωνσταντίνος

Αναπληρωτής Καθηγητής

Τριμελής Εξεταστική Επιτροπή

(υπογραφή) (υπογραφή) (υπογραφή)

Ευχαριστίες

Η παρούσα μεταπτυχιακή διπλωματική εργασία εκπονήθηκε στο πλαίσιο του ΠΜΣ «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων/Ασφάλεια Ψηφιακών Συστημάτων» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά.

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα, Αναπληρωτή Καθηγητή κ. Κωνσταντίνο Λαμπρινουδάκη, τόσο για την εμπιστοσύνη που μου έδειξε αναθέτοντας μου την εκπόνηση της παρούσας διπλωματικής εργασίας και για την βοήθεια, τις συμβουλές και την καθοδήγηση του κατά την εκπόνηση της, όσο και για το σύνολο των πολύτιμων γνώσεων που μου πρόσφερε σε όλη τη διάρκεια των διαλέξεων των διδασκόμενων μαθημάτων του στο πλαίσιο του ΠΜΣ «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων/Ασφάλεια Ψηφιακών Συστημάτων».

Ευχαριστώ επίσης όλους του καθηγητές του προγράμματος μεταπτυχιακών σπουδών «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων/Ασφάλεια Ψηφιακών Συστημάτων» για την προσφορά των γνώσεων τους, μέσα στα πλαίσια της εκπαίδευσης, στο εξειδικευμένο πεδίο της ασφάλειας ψηφιακών συστημάτων.

Παράλληλα, θα ήθελα να ευχαριστήσω τον Ελληνικό Στρατό για την ευκαιρία που μου πρόσφερε να διευρύνω τις γνώσεις μου σε έναν τόσο εξειδικευμένο τομέα, αυτών της ασφάλειας ψηφιακών συστημάτων.

Αφιερώνω την παρούσα διπλωματική εργασία στους γονείς μου και στην αδελφή μου.

Ιωάννης Κολόμβος

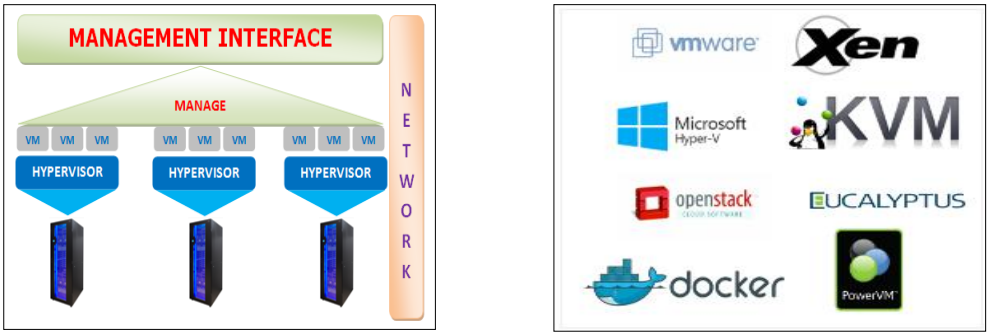
Πειραιάς, Μάρτιος 2017

Περίληψη

Στις μέρες μας μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing systems) βασίζονται στην εικονικοποίηση (virtualization). Στην επιστήμη της πληροφορικής, η εικονικοποίηση (virtualization) είναι ένας ευρύς όρος των υπολογιστικών συστημάτων που αναφέρεται σε έναν μηχανισμό αφαίρεσης, στοχευμένο στην απόκρυψη τόσο των λεπτομερειών της υλοποίησης της όσο και της κατάστασης των υπολογιστικών πόρων. Η εν λόγω αφαίρεση μπορεί είτε να αναγκάζει έναν πόρο να συμπεριφέρεται ως πλειάδα πόρων (π.χ. μία συσκευή αποθήκευσης σε διακομιστή τοπικού δικτύου), ή πολλαπλούς πόρους να συμπεριφέρονται ως ένας (π.χ. συσκευές αποθήκευσης σε κατανεμημένα συστήματα) **[1]**. Ωστόσο, η εικονικοποίηση (virtualization) έχει ευπάθειες και κατ᾽ επέκταση απειλές με αποτέλεσμα να εισάγει ένα πρόσθετο επίπεδο κινδύνου στα συστήματα υπολογιστικού νέφους (cloud computing systems).

Βασικός σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη της εικονικοποίησης (virtualization) μέσα σε περιβάλλοντα υπολογιστικού νέφους (cloud computing) με στόχο να εξεταστούν και να καταγραφούν οι ευπάθειες και οι απειλές που αυτή αντιμετωπίζει. Επιπλέον, θα διερευνηθούν και θα παρουσιαστούν τα μέτρα ασφαλείας που πρέπει να υιοθετούνται από τα συστήματα υπολογιστικού νέφους (cloud computing systems) για την αποφυγή και την εξάλειψη των απειλών της εικονικοποίησης (virtualization). Τέλος, θα επιχειρήσουμε μέσω της εφαρμογής καλών πρακτικών ασφαλείας σε όλα τα συστατικά στοιχεία που απαρτίζουν την εικονικοποίηση (virtualization), τα οποία είναι ο hypervisor, η διεπαφή διαχείρισης (management interface), οι εικονικές μηχανές (virtual machines) και το εικονικό δίκτυο επικοινωνίας (virtual network), να οδηγηθούμε σε υψηλά επίπεδα ασφαλείας της αρχιτεκτονικής εικονικοποίησης (virtualization) της **Εικόνα 1**, στην οποία βασίζει τη λειτουργία του μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing). Δεν θα επεκταθούμε καθόλου στην ασφάλεια του φυσικού υλικού και του λειτουργικού συστήματος του μηχανήματος υποδοχής

(host operating system) καθώς αυτά είναι μέρος «συμβατικών» μέτρων προστασίας και «συμβατικών» καλών πρακτικών ασφαλείας.



Εικόνα 1 - Αρχιτεκτονική Εικονικοποίησης (Virtualization) [41], [42]

Λέξεις Κλειδιά

Εικονικοποίηση (virtualization), υπολογιστικό νέφος (cloud computing), μηχάνημα υποδοχής (host machine), ιδεατή ή εικονική μηχανή (virtual machine), hypervisor ή VMM, λειτουργικό σύστημα μηχανήματος υποδοχής (host operating system), λειτουργικό σύστημα επισκέπτη (guest operating system), operating system level virtualization ή containers, ευπάθειες, απειλές, μέτρα ασφαλείας, αρχιτεκτονική εικονικοποίησης, διεπαφή διαχείριση (management interface), εικονικό δίκτυο επικοινωνίας (virtual network)

Abstract

Nowadays, most cloud computing systems are based on virtualization. In computer science, virtualization is a broad term of computing systems and it refers to an abstraction mechanism, which aims to hide both the details of the virtualization implementation and the state of computational resources. This abstraction can cause either a resource to act as a plurality of resources (e.g. a storage device to local network server) or multiple resources to act as one (e.g. storage devices in distributed systems) **[1]**. However, virtualization has vulnerabilities and threats and for this reason, it introduces an additional level of risk in cloud computing systems.

The main purpose of this thesis is the study of virtualization within cloud computing environments in order to examine and record the vulnerabilities and the threats that virtualization faces. Furthermore, we will investigate the security measures, which must be adopted by cloud computing systems, so as to prevent and eliminate the threats of virtualization. Finally, we will attempt through the application of best security practices to all of the components of virtualization, which are the hypervisor, the management interface, the virtual machines and the virtual network, to achieve high level of security for the virtualization architecture, which is depicted in **Figure 1.** The operation of most cloud computing systems is based on this architecture. We will not refer to the security of physical assets (hardware) and host machine operating system since these are part of conventional security measures and conventional best security practices.

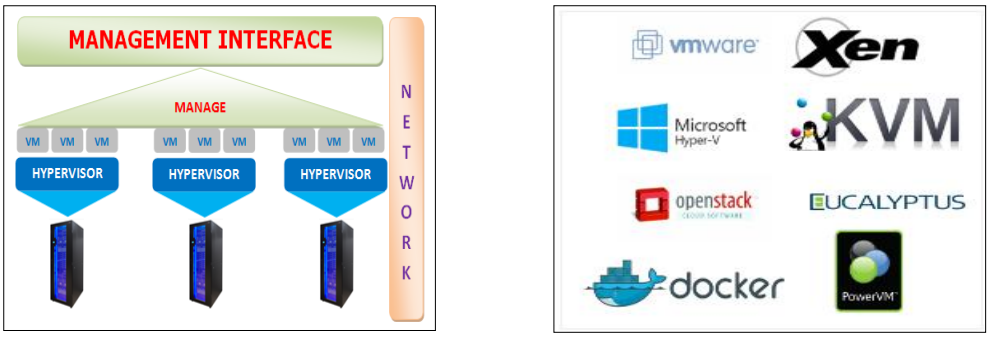


Figure 1 - Virtualization Architecture [41], [42]

Key Words

Virtualization, cloud computing, host machine, virtual machine, hypervisor or VMM, host operating system, guest operating system, operating system level virtualization or containers, vulnerabilities, threats, security measures, virtualization architecture, management interface, virtual network

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Συντομογραφίες

VMM	Virtual Machine Monitor
VM	Virtual Machine
ASP	Application Service Provider
VDI	Virtual Desktop Infrastructure
SAN	Storage Area Network
MMU	Memory Management Unit
TLB	Translation Loookaside Buffer
DoS	Denial of Service
VMBRs	VM-Based Rootkits
ARP	Address Resolution Protocol
MAC	Media Access Control
IDPS	Intrusion Detection and Prevention Systems
EKM	Encryption and Key Management
IDPS	Intrusion Detection and Prevention System
VF	Virtual Firewall
TVDs	Trusted Virtual Domains
ACMs	Access Control Mechanisms
vTPM	Virtual Trusted Platform Module
SLA	Service Level Agreement
Mac	Mandatory Access Control
DAC	Discretionary Access Control
RBAC	Role Based Access Control
EK	Endorsement Key
SRK	Storage Root Key
API	Application Programming Interface
CLI	Command-Line Interfaces
SDN	Software-Defined Network
SSH	Secure Shell
PAM	Pluggable Authentication Module
TLS	Transport Layer Security

SSL	Secure Socket Layer
MITM	Man in the Middle
NTP	Network Time Protocol
VPN	Virtual Private Network
vNIC	Virtual Network Interface Controller
DMZ	Demilitarized Zone
VLANs	Virtual Local Area Networks

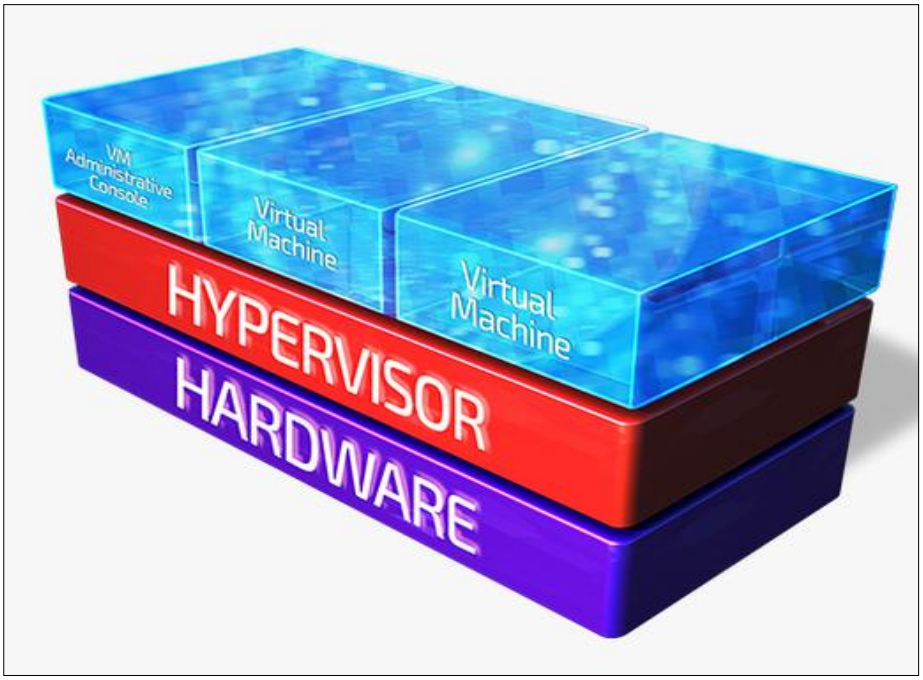
1

Εισαγωγή

Παρά το γεγονός ότι η εικονικοποίηση (virtualization) δεν είναι νέα τεχνολογία, ο τρόπος με τον οποίο χρησιμοποιείται σε σύγχρονες αρχιτεκτονικές υπολογιστικών συστημάτων παρέχει μια ισχυρή πλατφόρμα για την οικοδόμηση τους. Τα πλεονεκτήματα της εικονικοποίησης (virtualization) έχουν φανεί τα τελευταία χρόνια λόγω της ταχείας ανάπτυξης εμπορικών υπολογιστικών συστημάτων υλικού και λογισμικού που λειτουργούν σε περιβάλλοντα υπολογιστικού νέφους (cloud computing). Ουσιαστικά η εικονικοποίηση (virtualization) είναι ένα πλαίσιο, μεθοδολογία ή τεχνική που επιτυγχάνει τον διαμερισμό των φυσικών πόρων ενός υπολογιστή σε πολλαπλά περιβάλλοντα εκτέλεσης, εφαρμόζοντας μία ή περισσότερες τεχνολογίες όπως διαμερισμό σε επίπεδο υλικού ή σε επίπεδο λογισμικού, διαμερισμό σε επίπεδο χρόνου, μερική ή ολική προσομοίωση μηχανής, εξομοίωση, ποιότητα υπηρεσιών, και άλλα.

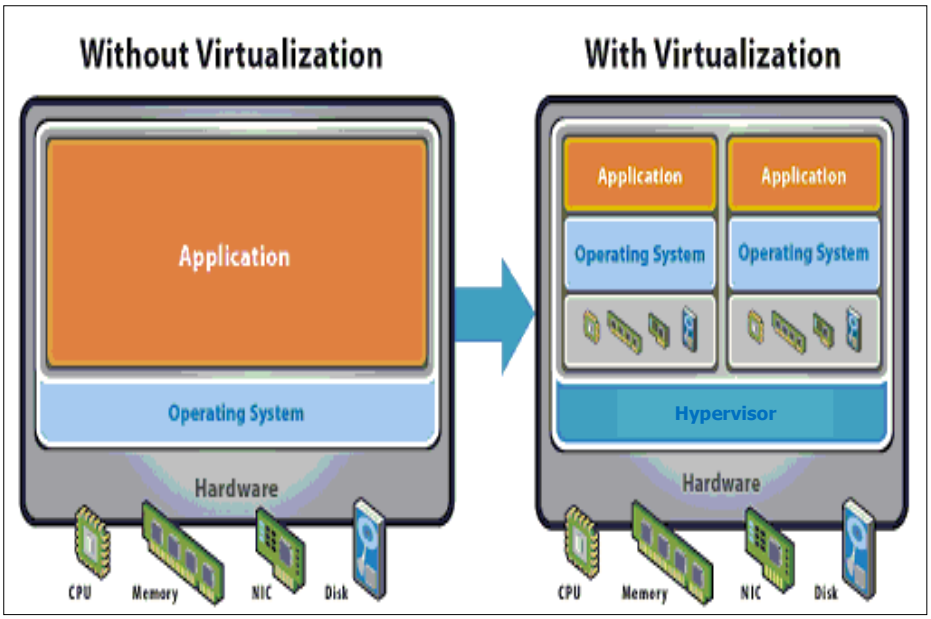
Η εικονικοποίηση (virtualization) περιλαμβάνει ένα στρώμα λειτουργικού που λειτουργεί σαν κάψουλα (encapsulating software layer), το οποίο ονομάζεται Hypervisor ή Virtual Machine Monitor (VMM). Το στρώμα αυτό περιβάλει ή βρίσκεται πίσω από ένα λειτουργικό σύστημα και παρέχει τις ίδιες εισόδους (input), εξόδους (output) και συμπεριφορά με αυτά που θα αναμενόταν και από μια πραγματική φυσική συσκευή. Αυτός ο αφαιρετικός μηχανισμός σημαίνει ότι ένας ιδανικός Hypervisor πρέπει να παρέχει στο λογισμικό ένα λογικό περιβάλλον ισοδύναμο με αυτό του συστήματος υποδοχής (host system) και παράλληλα το λογισμικό πρέπει να είναι αποσυνδεδεμένο από την κατάσταση του φυσικού υλικού (hardware) **[2]**. Το αφαιρετικό αυτό στρώμα επιτρέπει σε πολλαπλά ιδεατά μηχανήματα (virtual

machines), με ετερογενή λειτουργικά συστήματα να λειτουργούν το καθένα ξεχωριστά μέσα σε ένα απομονωμένο περιβάλλον, το ένα δίπλα στο άλλο, πάνω στο ίδιο φυσικό μηχάνημα, όπως φαίνεται στην **Εικόνα 2**.



Εικόνα 2 - Εικονικοποίηση (Virtualization) [43]

Η εικονικοποίηση (virtualization), λοιπόν, είναι ο διαμερισμός ενός φυσικού συστήματος σε πολλαπλά απομονωμένα μεταξύ τους εικονικά περιβάλλοντα. Τα εικονικά αυτά περιβάλλοντα συνήθως ονομάζονται virtual private servers, αλλά μπορεί κανείς να τα συναντήσει και με το όνομα partitions, guests, instances, containers, emulations ή virtual machines. Πολλαπλά ιδεατά μηχανήματα (virtual machines) μπορούν να μοιράζονται τους ίδιους φυσικούς πόρους χωρίς το ένα να επηρεάζει το άλλο, έτσι ώστε να μπορούν με ασφάλεια να τρέξουν πολλαπλά λειτουργικά συστήματα και εφαρμογές παράλληλα σε έναν υπολογιστή, μοιράζοντας τον ουσιαστικά σε πολλούς ιδεατούς υπολογιστές (virtual machines), όπως φαίνεται και στην **Εικόνα 3**.



Εικόνα 3 - Εικονικά Μηχανήματα (Virtual Machines) Πριν και Μετά την Εφαρμογή της Εικονικοποίηση (Virtualization) [44]

Η εικονικοποίηση (virtualization) έχει εγγενή πλεονεκτήματα ασφαλείας καθώς η παρουσία του Hypervisor συμβάλλει στην αποσύνδεση μεταξύ της λογικής και της φυσικής κατάστασης του υλικού. Από την άλλη πλευρά όμως, ο σχεδιασμός, η υλοποίηση και η ανάπτυξη της συγκεκριμένης τεχνολογίας έχει εισάγει νέες απειλές και θέματα ασφάλειας. Παραδείγματος χάριν, η αντίστροφη μηχανική (reverse engineering) μπορεί να επιτευχθεί ευκολότερα λόγω της δυνατότητας ενδοσκόπησης του συστήματος με αποτέλεσμα κλειδιά κρυπτογράφησης, αλγόριθμοι ασφαλείας, προστασία χαμηλού επιπέδου (low-level protection), συστήματα ανίχνευσης εισβολών και μέτρα anti-debugging να μπορούν να τεθούν ευκολότερα σε κίνδυνο. Επιπλέον, συναφείς τεχνολογίες όπως η εικονική δρομολόγηση (virtual routing) και δικτύωση (virtual networking) μπορούν να παραβιαστούν και να θέσουν την ασφάλεια του συστήματος σε κίνδυνο.

1.1. Στόχος Διπλωματικής Εργασίας

Στην παρούσα εργασία θα εξετάσουμε τις ευπάθειες και τις απειλές της εικονικοποίησης (virtualization) και θα διερευνήσουμε τα μέτρα ασφαλείας για την αντιμετώπιση των απειλών της με στόχο την βέλτιστη προστασία των συστημάτων υπολογιστικού νέφους (cloud computing systems), τα οποία βασίζονται στην εικονικοποίηση (virtualization). Τέλος, θα επιχειρήσουμε μέσω της εφαρμογής καλών πρακτικών ασφαλείας σε όλα τα συστατικά στοιχεία που αποτελούν την εικονικοποίηση (virtualization), τα οποία είναι ο hypervisor, η διεπαφή διαχείριση (management interface), οι εικονικές μηχανές (virtual machines) και το εικονικό δίκτυο επικοινωνίας (virtual network), να οδηγηθούμε σε υψηλά επίπεδα ασφαλείας της αρχιτεκτονικής εικονικοποίησης (virtualization) της **Εικόνα 1**, στην οποία βασίζει την λειτουργία του μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing). Δεν θα επεκταθούμε καθόλου στην ασφάλεια του φυσικού υλικού και του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) καθώς αυτά είναι μέρος «συμβατικών» μέτρων προστασίας και «συμβατικών» καλών πρακτικών ασφαλείας.

1.2. Δομή της Εργασίας

Το υπόλοιπο της διπλωματικής εργασίας είναι δομημένο ως εξής. Στο Κεφάλαιο 2 γίνεται μία ανάλυση της έννοιας του υπολογιστικού νέφους (cloud computing) και των μοντέλων υπηρεσιών και ανάπτυξης αυτού. Στην συνέχεια, αναλύεται η έννοια της εικονικοποίησης (virtualization) και ο τρόπος υλοποίησης της με την τεχνική hardware virtualization και δίνεται σύντομη περιγραφή του hypervisor και των τύπων του, της ιδεατής ή εικονικής μηχανής (virtual machine), του μηχανήματος υποδοχής (host machine), των τρόπων υλοποίησης hardware virtualization καθώς και περιγραφή και άλλων τεχνικών που χρησιμοποιούνται στην εικονικοποίηση (virtualization). Επιπλέον, γίνεται ανάλυση του επιπέδου ασφάλειας της εικονικοποίησης

(virtualization) με σκοπό να εισάγει τον αναγνώστη στη λεπτομερή ανάλυση των ευπαθειών και απειλών της που ακολουθεί στο Κεφάλαιο 3, καθώς και των μέτρων ασφαλείας για την αντιμετώπιση αυτών που ακολουθεί στο Κεφάλαιο 4. Τέλος, περιγράφεται ο τρόπος υλοποίησης της εικονικοποίησης (virtualization) με την τεχνική operating system level virtualization ή containers και δίδεται μία σύντομη ανάλυση της ασφάλειας της.

Στο Κεφάλαιο 3 εξετάζονται οι ευπάθειες που παρουσιάζει ένα σύστημα υπολογιστικού νέφους (cloud computing system) όταν εφαρμόζεται σε αυτό η τεχνολογία της εικονικοποίησης (virtualization). Για κάθε κατηγορία ευπαθειών καταγράφονται και οι αντίστοιχες απειλές. Μέσα σε αυτό το πλαίσιο, λοιπόν, οι ευπάθειες και οι απειλές των συστημάτων υπολογιστικού νέφους (cloud computing systems) που βασίζονται στην εικονικοποίηση (virtualization) μπορούν να ταξινομηθούν σε τέσσερις κατηγορίες:

- Ευπάθειες και απειλές του hypervisor, όπως αυτές αναλύονται στις ενότητες 3.1., 3.2., 3.3. και 3.4. παρακάτω.
- Ευπάθειες και απειλές των εικονικών μηχανών (virtual machines), όπως αυτές αναλύονται στις ενότητες 3.5., 3.6., 3.7., 3.8. και 3.9. παρακάτω.
- Ευπάθειες και απειλές του δικτύου επικοινωνίας (network communication), όπως αυτές αναλύονται στις ενότητες 3.10. και 3.11. παρακάτω.
- Ευπάθειες και απειλές του τρόπου διαμόρφωσης (configuration) του συστήματος, όπως αυτές αναλύονται στις ενότητες 3.12. και 3.13. παρακάτω.

Στο Κεφάλαιο 4 παρουσιάζονται τα μέτρα ασφαλείας που πρέπει να υιοθετούνται από τα συστήματα υπολογιστικού νέφους (cloud computing system) όταν εφαρμόζεται σε αυτά η τεχνολογία της εικονικοποίησης (virtualization) με στόχο την αποφυγή και αν είναι δυνατόν την εξάλειψη των απειλών της εικονικοποίησης (virtualization). Αρχικά στην ενότητα 4.1. αναλύονται τα γενικά μέτρα ασφαλείας και στην συνέχεια στις ενότητες από 4.2. μέχρι 4.14. αναλύονται πιο συγκεκριμένα τα μέτρα ασφαλείας που πρέπει να εφαρμόζονται για κάθε μία ευπάθεια και αντίστοιχη απειλή, οι οποίες θα αναλυθούν στο Κεφάλαιο 3. Τέλος, στον **Πίνακας 2** παρουσιάζεται μία αντιστοίχιση των ευπαθειών με τις απειλές που αυτές προκαλούν και τα

αντίστοιχα μέτρα ασφαλείας που πρέπει να υιοθετηθούν για την εξάλειψη τους.

Στο Κεφάλαιο 5 θα ασχοληθούμε με το στρώμα της εικονικοποίησης (virtualization) της αρχιτεκτονικής υπολογιστικού νέφους (cloud computing) και των τμημάτων που το απαρτίζουν, τα οποία είναι ο hypervisor, η διεπαφή διαχείρισης (management interface), οι εικονικές μηχανές (virtual machines) και το εικονικό δίκτυο επικοινωνίας (virtual network). Ο στόχος είναι μέσω της εφαρμογής καλών πρακτικών ασφαλείας, για όλα τα μέρη που αποτελούν την εικονικοποίηση (virtualization), να οδηγηθούμε σε υψηλά επίπεδα ασφαλείας της αρχιτεκτονικής εικονικοποίησης (virtualization) της **Εικόνα 1**, στην οποία βασίζει την λειτουργία του μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing). Δεν θα επεκταθούμε καθόλου στην ασφάλεια του φυσικού υλικού και του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) καθώς αυτά είναι μέρος «συμβατικών» μέτρων προστασίας και «συμβατικών» καλών πρακτικών ασφαλείας.

Τέλος, στο Κεφάλαιο 6 θα κλείσουμε τη διπλωματική εργασία με την περίληψη των όσων αναλύθηκαν καθώς και με τα συμπεράσματα της έρευνας μας. Επιπλέον, θα προταθεί, ως μελλοντική εργασία, η διεξαγωγή ανάλογης έρευνας για την μελέτη και καταγραφή των ευπαθειών και απειλών, των μέτρων ασφαλείας και των καλών πρακτικών ασφαλείας της αρχιτεκτονικής για την υλοποίηση της εικονικοποίησης (virtualization) με την τεχνική operating system level virtualization ή containers.

2

Ορισμοί – Βασικές Έννοιες

Σε αυτό το Κεφάλαιο θα αναλύσουμε την έννοια του υπολογιστικού νέφους (cloud computing) και των μοντέλων υπηρεσιών και ανάπτυξης αυτού. Στην συνέχεια, θα αναλύσουμε την έννοια της εικονικοποίησης (virtualization) και τον τρόπο υλοποίησης της με την τεχνική του hardware virtualization και θα ακολουθήσει σύντομη περιγραφή του hypervisor και των τύπων του, της ιδεατής ή εικονικής μηχανής (virtual machine), του μηχανήματος υποδοχής (host machine), των τρόπων υλοποίησης hardware virtualization καθώς και περιγραφή και άλλων τεχνικών που μπορούν να αξιοποιηθούν. Επιπλέον, θα γίνει μία ανάλυση της ασφάλειας της εικονικοποίησης (virtualization) με σκοπό να εισάγει τον αναγνώστη στη λεπτομερή ανάλυση των ευπαθειών και απειλών της που θα ακολουθήσει στο Κεφάλαιο 3, καθώς και των μέτρων ασφαλείας για την αντιμετώπιση αυτών που θα ακολουθήσει στο Κεφάλαιο 4. Τέλος, θα περιγράψουμε τον τρόπο υλοποίησης της εικονικοποίησης (virtualization) με την τεχνική operating system level virtualization ή containers και θα γίνει μία σύντομη μελέτη της ασφάλειας της.

2.1. Υπολογιστικό Νέφος (Cloud Computing)

Αυτό που σήμερα ονομάζουμε υπολογιστικό νέφος (cloud computing), είναι η συνέχεια του πεπαλαιωμένου ASP (Application Service Provider). Πιο συγκεκριμένα, με τον όρο ASP νοείται μια εφαρμογή παροχής υπηρεσιών. Είναι μια εφαρμογή η οποία παρέχει υπηρεσίες σε πελάτες μέσω δικτύου, όπως η πρόσβαση σε μια συγκεκριμένη εφαρμογή λογισμικού (όπως η

διαχείριση πελατειακών σχέσεων), χρησιμοποιώντας ένα τυποποιημένο πρωτόκολλο (όπως το HTTP).

Το σύγχρονο νέφος (cloud) ενσωματώνει τεχνολογίες οι οποίες στο ASP δεν υφίσταντο. Η κύρια διαφορά είναι πως το νέφος (cloud) δεν ανήκει σε κάποιον, εν' αντιθέσει με παλιές εφαρμογές ASP. Σε αυτήν την περίπτωση μισθώνεις τη χρήση του χώρου που αποκτάς και είσαι ιδιοκτήτης των δεδομένων σου και μόνο αυτών. Οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετούν πολλαπλούς χρήστες με τη χρήση του μοντέλου πολλαπλών μισθωτών (multi-tenant), με τους διάφορους φυσικούς και εικονικούς πόρους να ανατίθενται δυναμικά και εκ νέου ανάλογα με τη ζήτηση των καταναλωτών. Υπάρχει μια αίσθηση ανεξαρτησίας από τον τόπο καθώς ο χρήστης δεν έχει κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να προσδιορίζει την τοποθεσία σ' ένα υψηλότερο επίπεδο (πχ. χώρα, κράτος, ή datacenter).

Παραδείγματα πόρων αποτελούν:

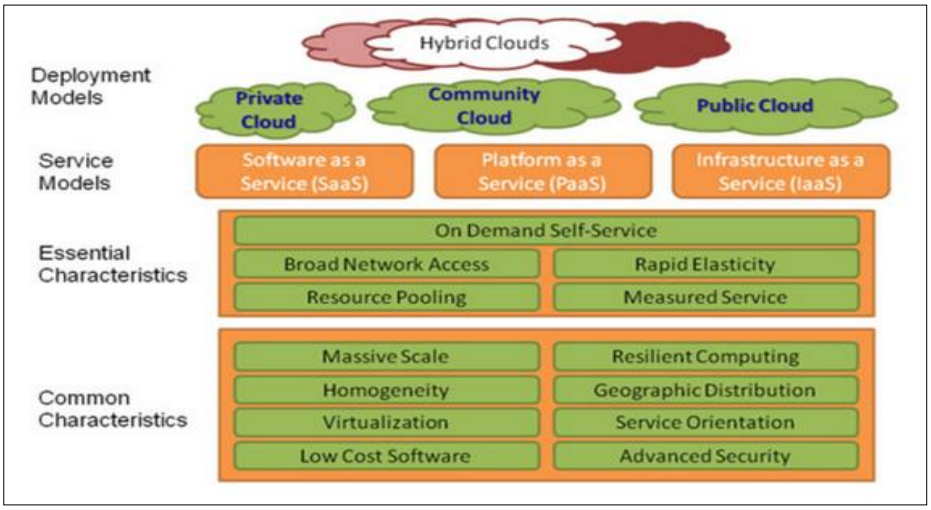
- Οι αποθηκευτικοί χώροι.
- Η επεξεργασία.
- Η μνήμη.
- Το εύρος ζώνης (bandwidth) του δικτύου.
- Καθώς και οι εικονικές μηχανές.

Ένας χρήστης έχει τη δυνατότητα να δεσμεύσει τους υπολογιστικούς πόρους που του χρειάζονται, όπως για παράδειγμα χρόνο στον εξυπηρετητή και αποθηκευτικό χώρο στο δίκτυο. Οι παραπάνω δυνατότητες λαμβάνουν χώρα ανάλογα με τις ανάγκες του χρήστη, αυτόματα χωρίς να απαιτείται ανθρώπινη διαμεσολάβηση με το φορέα παροχής κάθε υπηρεσίας. Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών που προωθούν την χρήση από ετερογενείς thin ή thick client πλατφόρμες (π.χ. κινητά τηλέφωνα, φορητούς υπολογιστές και PDAs).

Ένα σημαντικό πλεονέκτημα είναι πως το νέφος (cloud) διαθέτει εικονικοποίηση (virtualization). Με την χρησιμοποίηση του νέφους (cloud)

επιτυγχάνεται η εξοικονόμηση των πόρων, καθώς ο καθένας χρησιμοποιεί μόνο ότι και όποτε θέλει. Υπάρχει η δυνατότητα οι πόροι να δεσμεύονται για χρήση γρήγορα, ελαστικά και αυτόματα, έτσι ώστε να εμφανίζονται στιγμιαία ως μη διαθέσιμοι και επίσης να αποδεσμεύονται ώστε να εμφανιστούν ξανά ως διαθέσιμοι. Για τον χρήστη, οι διαθέσιμες επιλογές για δέσμευση και χρήση συχνά φαίνεται να είναι απεριόριστες και μπορούν να αγοραστούν ανά πάσα στιγμή και σε οποιαδήποτε ποσότητα, αναλόγως πάντα προς την αγοραστική δυνατότητα του χρήστη **[3]**.

Το νέφος (cloud) αποτελεί, λοιπόν, ένα μοντέλο που επιτρέπει την κατά-ζήτηση (on- demand) πρόσβαση μέσω δικτύου σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (δίκτυα, εξυπηρετητές, μνήμη, εφαρμογές και υπηρεσίες) που μπορούν να προσφερθούν με ελάχιστη προσπάθεια διαχείρισης ή με αλληλεπίδραση με τον πάροχο της υπηρεσίας. Αυτό το μοντέλο προωθεί την διαθεσιμότητα, και αποτελείται από πέντε απαραίτητα χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης **[4]**, όπως φαίνεται και στην **Εικόνα 4**.

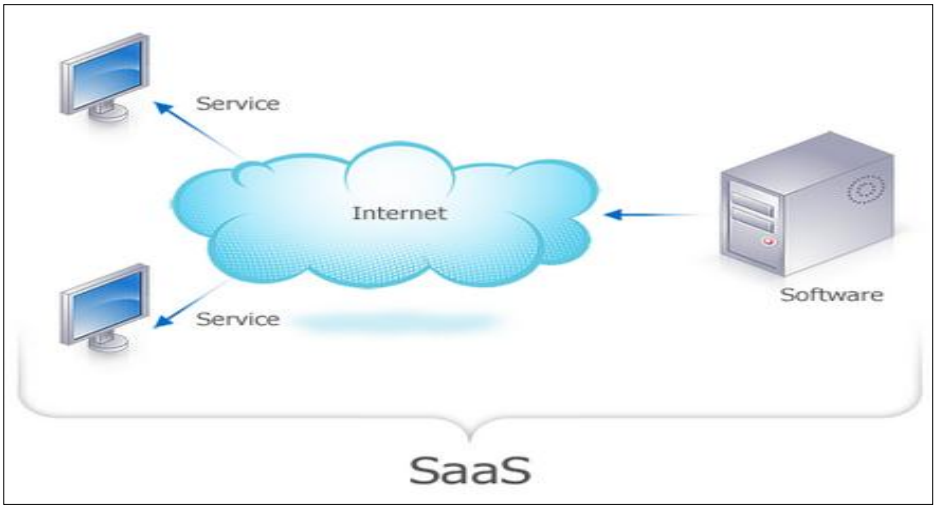


Εικόνα 4 - Αρχιτεκτονική Υπολογιστικού Νέφους (Cloud Computing) [45]

2.1.1. Μοντέλα Υπηρεσιών

2.1.1.1. Νέφος Λογισμικού ως μια Υπηρεσία (Cloud Software as a Service, SaaS)

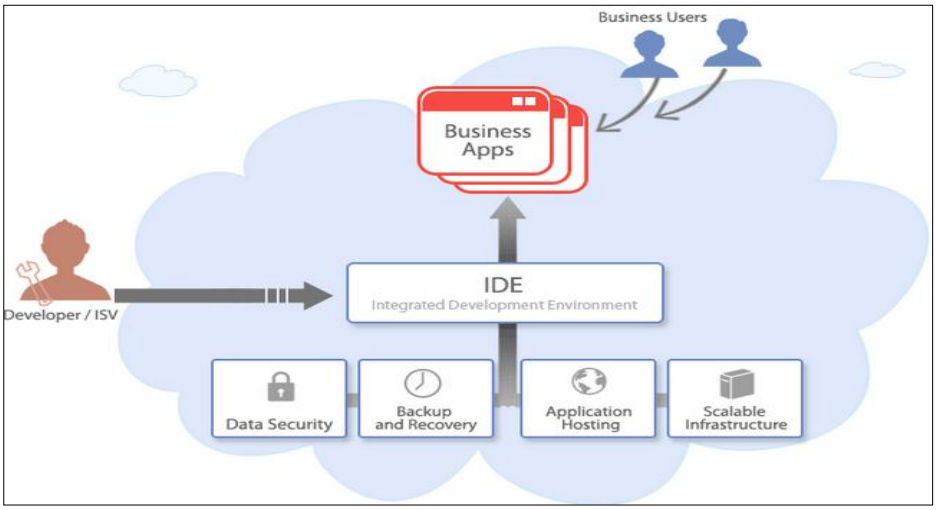
Η δυνατότητα που παρέχεται στον χρήστη είναι να χρησιμοποιεί τις εφαρμογές του παρόχου που εδράζονται σε μια υποδομή νέφους (cloud). Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές χρήστη μέσα από διεπαφές (interfaces) ή εργαλεία, όπως ένα πρόγραμμα περιήγησης στο Web (web browser). Ένα αντιπροσωπευτικό παράδειγμα, ώστε να γίνει αντιληπτό το ανωτέρω, είναι το GoogleDrive και οι εφαρμογές που μπορούν να εκτελεστούν απ' ευθείας σε αυτό. Ο χρήστης δεν έχει τη διαχείριση ή τον έλεγχο του χρησιμοποιούμενου νέφους (cloud) συμπεριλαμβανομένων των δικτύων, των διακομιστών (servers), των λειτουργικών συστημάτων, των αποθηκευτικών μονάδων ή ακόμα και μεμονωμένων δυνατοτήτων της εφαρμογής. Ο χρήστης, λοιπόν, δεν χρειάζεται να κατανοήσει και να μπορεί να υποστηρίζει τη φιλοσοφία της υπηρεσίας αλλά μόνο να μπορεί να τη χρησιμοποιήσει μέσα από τη διεπαφή που διαθέτει.



Εικόνα 5 – Αρχιτεκτονική Cloud Software as a Service [46]

2.1.1.2. Νέφος Πλατφόρμας ως μια Υπηρεσία (Cloud Platform as a Service, PaaS)

Η δυνατότητα που παρέχεται στον χρήστη είναι να αναπτύσσει στο νέφος (cloud), εφαρμογές που είτε έχει δημιουργήσει ο ίδιος ή έχει αποκτήσει και οι οποίες έχουν δημιουργηθεί με χρήση γλωσσών προγραμματισμού και εργαλείων που υποστηρίζονται από τον πάροχο. Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποκείμενη υποδομή, συμπεριλαμβανομένου του δικτύου, των διακομιστών (servers), των λειτουργικών συστημάτων, της μνήμης και των αποθηκευτικών μέσων, αλλά έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί και πιθανώς τον έλεγχο κάποιων ρυθμίσεων του περιβάλλοντος φιλοξενίας των εφαρμογών.

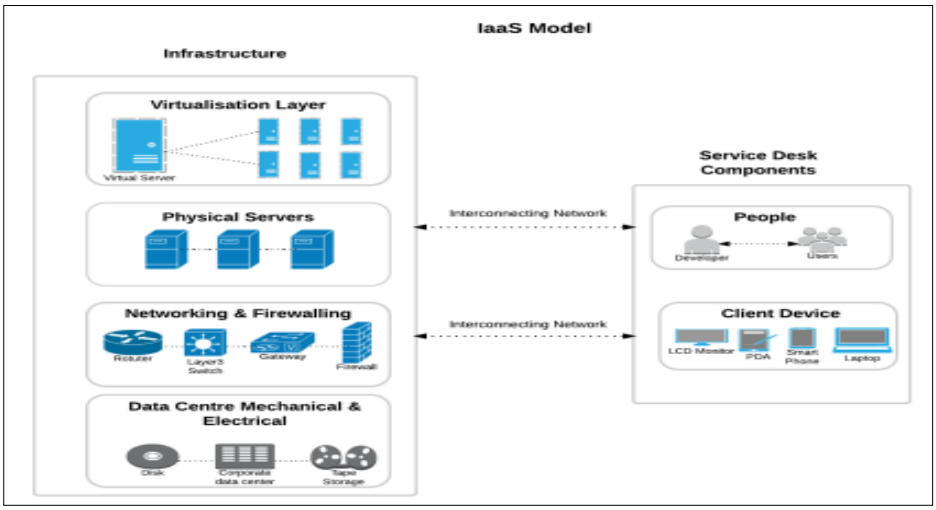


Εικόνα 6 – Αρχιτεκτονική Cloud Platform as a Service [47]

2.1.1.3. Νέφος Υποδομής ως μια Υπηρεσία (Cloud Infrastructure as a Service, IaaS)

Η δυνατότητα που παρέχεται στον χρήστη είναι να μπορεί να δεσμεύσει προς χρήση επεξεργαστική ισχύ, αποθηκευτικά μέσα, δίκτυα, και άλλους θεμελιώδεις υπολογιστικούς πόρους. Αφού, λοιπόν, ο χρήστης δεσμεύσει τους αναγκαίους πόρους είναι σε θέση να αναπτύξει κατά βούληση και να εκτελέσει αυθαίρετο λογισμικό, το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα

και εφαρμογές. Ο χρήστης δεν έχει τη διαχείριση ή τον έλεγχο του χρησιμοποιούμενου νέφους (cloud), αλλά έχει τον έλεγχο των λειτουργικών συστημάτων, των αποθηκευτικών μέσων, των εφαρμογών που έχουν αναπτυχθεί και πιθανόν περιορισμένο έλεγχο σε κάποιους διαδικτυακού πόρους, όπως για παράδειγμα σε τείχος προστασίας (firewall).



Εικόνα 7 – Αρχιτεκτονική Cloud Infrastructure as a Service [48]

2.1.2. Μοντέλα Ανάπτυξης

2.1.2.1. Ιδιωτικό Νέφος (Private Cloud)

Η υποδομή αυτή εξυπηρετεί αποκλειστικά ένα οργανισμό. Η διαχείρισή της μπορεί να γίνει είτε από τον ίδιο τον οργανισμό ή από κάποιον τρίτο και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

2.1.2.2. Δημόσιο Νέφος (Public Cloud)

Η υποδομή αυτή διατίθεται στο ευρύ κοινό ή σε μια μεγάλη ομάδα εταιρειών/επιχειρήσεων και ανήκει σε έναν οργανισμό, ο οποίος διαχειρίζεται και μισθώνει τις υπηρεσίες του νέφους (cloud).

2.1.2.3. Κοινοτικό Νέφος (Community Cloud)

Η υποδομή αυτή διαμοιράζεται σε διάφορους οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανάγκες. Η διαχείριση της υποδομής μπορεί να γίνεται είτε από τον ίδιο τον οργανισμό ή από κάποιον τρίτο και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

2.1.2.4. Υβριδικό Νέφος (Hybrid Cloud)

Η υποδομή αυτή είναι μια σύνθεση δύο ή περισσότερων νεφών (cloud) (ιδιωτικού, δημόσιου ή κοινοτικού) τα οποία παραμένουν μοναδικές οντότητες, διατηρούν δηλαδή τα στοιχεία της ανεξαρτησίας τους, αλλά συνάμα συνδέονται μεταξύ τους με τυποποιημένη ή αποκλειστική τεχνολογία, η οποία επιτρέπει τη φορητότητα δεδομένων και εφαρμογών (π.χ. εξισορρόπηση φόρτου εργασίας μεταξύ των νεφών (clouds)).

2.2. Εικονικοποίηση (Virtualization)

Με τον όρο εικονικοποίηση (virtualization) εννοούμε την τεχνολογία με την οποία τα φυσικά συστήματα μετατρέπονται σε ιδεατά (virtual machines). Κάθε φυσικός πόρος (επεξεργαστική ισχύς, μνήμη, δίκτυο, αποθηκευτικός χώρος κλπ.) γίνεται ένας ενιαίος πόρος και μοιράζεται ταυτόχρονα σε πολλά εικονικά συστήματα. Η εικονικοποίηση (virtualization) αποτελεί θεμελιώδη συστατικό στοιχείο του υπολογιστικού νέφους (cloud computing) και καθιστά εφικτό πολλαπλά λειτουργικά συστήματα και εφαρμογές να «τρέχουν» ταυτόχρονα στον ίδιο διακομιστή (server), αυξάνοντας έτσι την αξιοποίηση και την προσαρμοστικότητα των φυσικών πόρων. Με την χρήση της εικονικοποίησης (virtualization) επιτυγχάνουμε εξοικονόμηση χρόνου, χρημάτων, ενέργειας και υψηλή διαθεσιμότητα.

Στην ουσία, η εικονικοποίηση (virtualization) μας επιτρέπει να μετατρέψουμε το υλικό (hardware) σε λογισμικό (software). Μπορούμε, λοιπόν, με την χρήση της εικονικοποίησης (virtualization) να μετατρέψουμε τους φυσικούς πόρους ενός υπολογιστή σε εικονικούς (virtual), συμπεριλαμβανομένων των ΚΜΕ (CPU), Μνήμη (RAM), Σκληρό Δίσκο (hard disk) και Ελεγκτή Δικτύου (network controller), προκειμένου να δημιουργήσουμε ένα πλήρως λειτουργικό ιδεατό μηχάνημα (virtual machines) που μπορεί να «τρέχει» το δικό του λειτουργικό σύστημα και τις δικές του εφαρμογές ακριβώς όπως ένας «πραγματικός» υπολογιστής.

Πολλαπλά ιδεατά μηχανήματα (virtual machines) μπορούν να μοιράζονται τους φυσικούς πόρους ενός υπολογιστή χωρίς το ένα να επηρεάζει το άλλο. Με αυτό τον τρόπο μπορούμε με ασφάλεια να τρέξουμε πολλαπλά λειτουργικά συστήματα και εφαρμογές παράλληλα σε έναν υπολογιστή, μοιράζοντάς τον ουσιαστικά σε πολλούς ιδεατούς υπολογιστές (virtual machines), οι οποίοι λειτουργούν ο κάθε ένας ξεχωριστά μέσα σε ένα απομονωμένο περιβάλλον, όπως φαίνεται και στην **Εικόνα 3** παραπάνω. Αυτή η μέθοδος εικονικοποίησης (virtualization) υλοποιείται με την τεχνική hardware virtualization, η οποία διαφέρει από αυτή που περιγράφεται στην ενότητα 2.4., την υλοποίηση δηλαδή της εικονικοποίησης (virtualization) με την τεχνική operating system level virtualization ή containers. Τέλος, στις ενότητες 2.2.1., 2.2.2., 2.2.3., 2.2.4. και 2.2.5. που ακολουθούν αναλύονται το λογισμικό και οι τρόποι υλοποίησης της hardware virtualization.

2.2.1. Hypervisor ή Virtual Machine Monitor (VMM)

Ο Hypervisor είναι λογισμικό υπολογιστή, πλαισίου ή υλικού που δημιουργεί και διαχειρίζεται τις ιδεατές μηχανές (virtual machines). Η μηχανή στην οποία εγκαθίσταται ο hypervisor ονομάζεται μηχάνημα υποδοχής (host machine) ενώ οι ιδεατές μηχανές συνήθως καλούνται μηχανήματα επισκεπτών (guest machines) **[5]**. Στο πλαίσιο αυτό, ο hypervisor είναι ένα λογισμικό που επιτρέπει σε έναν υπολογιστή να υποστηρίζει πολλαπλά λογικά περιβάλλοντα

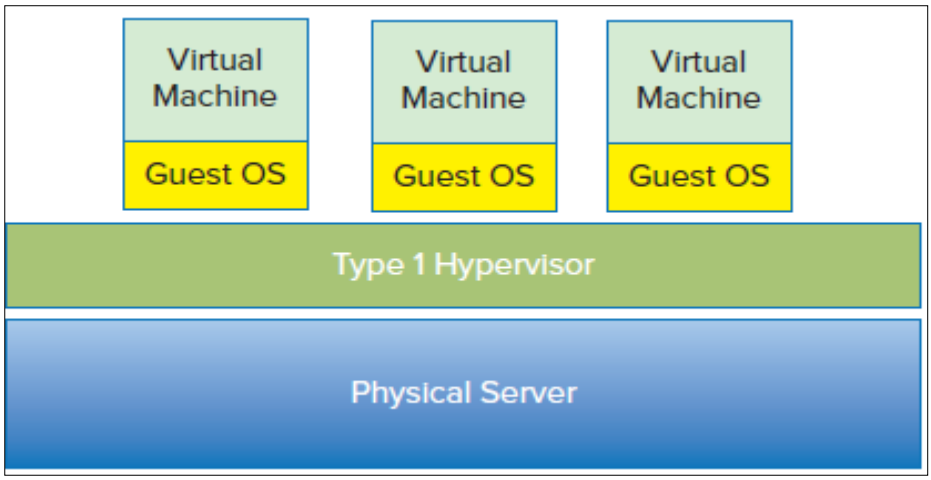
εκτέλεσης, με ετερογενή ή μη λειτουργικά συστήματα που λειτουργούν το καθένα ξεχωριστά μέσα σε ένα απομονωμένο περιβάλλον, το ένα δίπλα στο άλλο, πάνω στο ίδιο φυσικό μηχάνημα. Όλοι οι χρήστες βλέπουν τα συστήματά τους ως αυτοτελείς υπολογιστές, απομονωμένους από αυτούς των άλλων χρηστών, παρά το γεγονός ότι κάθε χρήστης εξυπηρετείται από το ίδιο φυσικό μηχάνημα.

2.2.2. Τύποι Hypervisor ή VMM

2.2.2.1. Τύπος 1, Native or Bare-metal Hypervisor ή VMM

Αυτού του τύπου ο Hypervisor εγκαθίσταται απευθείας πάνω στο φυσικό υλικό (physical hardware) του μηχανήματος υποδοχής (host) και ελέγχει το υλικό (hardware) και διαχειρίζεται τα λειτουργικά συστήματα των ιδεατών μηχανών (guest operating systems). Γι αυτό τον λόγο καλείται native ή bare metal hypervisor **[5]**, όπως φαίνεται και στην **Εικόνα 8**.

Το πιο σημαντικό χαρακτηριστικό του τύπου 1 hypervisor είναι ότι έχει καλύτερη απόδοση και χαμηλότερη επιβάρυνση στην λειτουργία του συστήματος συγκριτικά με τον τύπο 2 hypervisor, επιπλέον είναι πολύ «ελαφρύ» λογισμικό και εκτελείται στο υψηλότερο επίπεδο (highest level of privilege). Οι ποιο γνωστοί bare-metal hypervisors είναι οι VMware vSphere ESXi, Microsoft Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization (RHEV) και KVM.

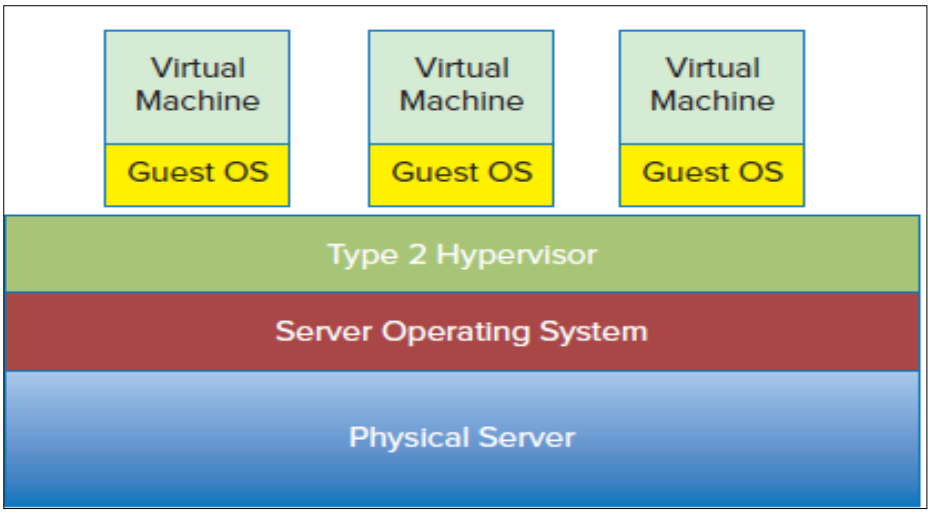


Εικόνα 8 - Native or Bare-metal Hypervisor ή VMM [49]

2.2.2.2. Τύπος 2, Hosted Hypervisor ή VMM

Αυτού του τύπου ο Hypervisor εγκαθίσταται αφού προηγουμένως έχει γίνει εγκατάσταση, σε έναν υπολογιστή, ενός λειτουργικού συστήματος. Ο τύπος 2 hypervisor είναι ουσιαστικά μία εφαρμογή του λειτουργικού συστήματος και λειτουργεί σαν ένα επίπεδο αφαίρεσης ανάμεσα στο λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) και στα λειτουργικά συστήματα των ιδεατών μηχανών (guest operating systems). Γι αυτό τον λόγο καλείται hosted hypervisor **[5]**, όπως φαίνεται και στην **Εικόνα 9**.

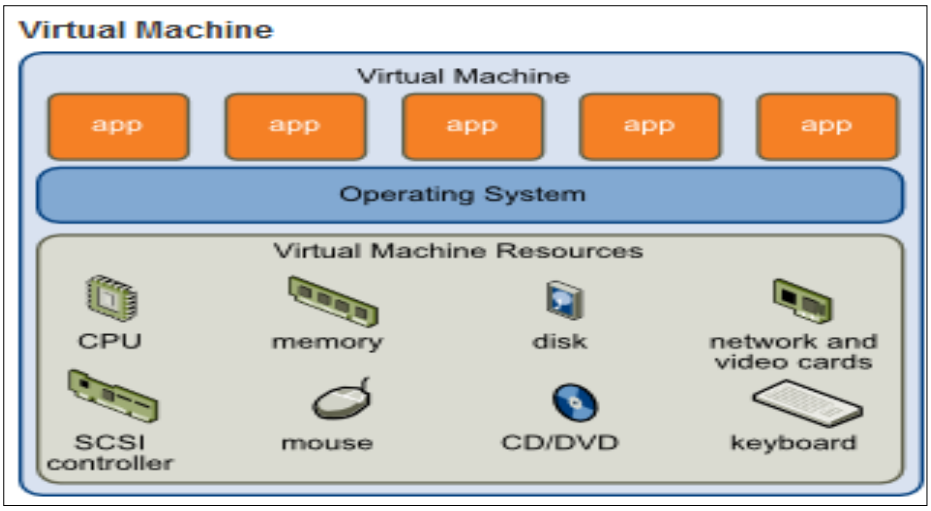
Ο τύπος 2 hypervisor είναι περισσότερο συμβατός με τις φυσικές συσκευές υλικού (physical hardware devices) συγκριτικά με τον τύπο 1 hypervisor. Οι ποιο γνωστοί hosted hypervisors είναι οι VMware Workstation, VMware Player, VirtualBox, Parallels Desktop για Mac και QUEM.



Εικόνα 9 - Hosted Hypervisor ή VMM [50]

2.2.3. Ιδεατή Μηχανή ή Εικονική Μηχανή (Virtual Machine)

Η ιδεατή μηχανή ή εικονική μηχανή (virtual machine) είναι μια εξομοίωση ενός ξεχωριστού υπολογιστή μέσα σε έναν φυσικό υπολογιστή, η οποία έχει το δικό της λειτουργικό σύστημα και εφαρμογές. Ένα ιδεατό μηχάνημα (virtual machine) είναι όπως ένα φυσικό μηχάνημα (physical machine), αλλά αντί για ηλεκτρονικά στοιχεία, αποτελείται από ένα σύνολο αρχείων λογισμικού. Κάθε ιδεατό μηχάνημα (virtual machine) είναι ένα ισχυρά απομονωμένο πακέτο λογισμικού και αντιπροσωπεύει ένα ολοκληρωμένο σύστημα με την δική του ΚΜΕ (CPU), μνήμη (RAM), σκληρό δίσκο (hard disk), κάρτα δικτύου (NIC) και BIOS, όπως φαίνεται στην **Εικόνα 10**.



Εικόνα 10 - Ιδεατή Μηχανή ή Εικονική Μηχανή (Virtual Machine) [51]

Το ιδεατό μηχάνημα (virtual machine) είναι ένα περιβάλλον ή λειτουργικό σύστημα, που δεν είναι φυσικά υπαρκτό αλλά δημιουργείται μέσα σε ένα άλλο περιβάλλον. Στο πλαίσιο αυτό, ένα ιδεατό μηχάνημα (virtual machine) ονομάζεται «guest» ενώ το περιβάλλον μέσα στο οποίο εκτελείται ονομάζεται «host». Τα ιδεατά μηχανήματα (virtual machines) δημιουργούνται συνήθως για να εκτελέσουν ένα σύνολο εντολών (instruction set) διαφορετικό από αυτό του περιβάλλοντος μέσα στο οποίο φιλοξενούνται (host). Επιπλέον, ένα host περιβάλλον μπορεί να εκτελεί πολλά ιδεατά μηχανήματα (virtual machines) ταυτόχρονα και να αναθέτει δυναμικά τους πόρους του στα ιδεατά μηχανήματα (virtual machines).

Ένας χρήστης που αλληλεπιδρά με ένα εικονικό μηχάνημα (virtual machine) το αντιλαμβάνεται σαν ένα φυσικό μηχάνημα υπό την έννοια ότι έχει πρόσβαση στους πόρους του εικονικού μηχανήματος (virtual machine), όπως στον σκληρό δίσκο, την μνήμη, τον επεξεργαστή και τις δικτυακές συνδέσεις. Στην πραγματικότητα, όλοι αυτοί οι πόροι του εικονικού μηχανήματος (virtual machine) είναι ιδεατοί. Για παράδειγμα, αντί να προσπελαύνει έναν πραγματικό σκληρό δίσκο, ο χρήστης προσπελαύνει μία δομή του host περιβάλλοντος. Αυτή η δομή στη συνέχεια προσπελαύνει το πραγματικό δίσκο για να καταγράψει τα δεδομένα.

2.2.4. Μηχάνημα Υποδοχής (Host Machine)

Το μηχάνημα υποδοχής (host machine) είναι το φυσικό μηχάνημα πάνω στο οποίο εγκαθίσταται ο hypervisor. Το μηχάνημα υποδοχής (host machine) παρέχει τους φυσικούς πόρους υλικού, όπως ΚΜΕ (CPU), μνήμη (RAM), σκληρό δίσκο (hard disk), κάρτα δικτύου (NIC) και οποιοδήποτε άλλο αναγκαίο πόρο για να λειτουργήσουν οι ιδεατές μηχανές (virtual machines).

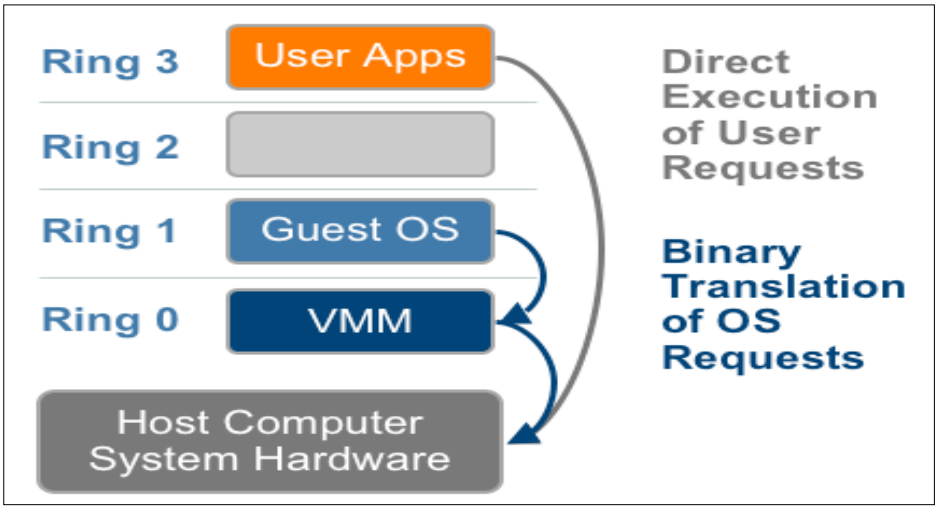
2.2.5. Τρόποι Υλοποίησης Hardware Εικονικοποίησης (Virtualization)

2.2.5.1. Πλήρης Εικονικοποίηση (Full Virtualization)

Η τεχνική της πλήρους εικονικοποίησης (Full Virtualization) έχει σχεδιαστεί έτσι ώστε να παρέχει πλήρη αποσύνδεση ανάμεσα στην φυσική και στην ιδεατή ή εικονική μηχανή (virtual machine), μέσα στην οποία εκτελείται το λειτουργικό σύστημα επισκέπτη (guest operating system). Επιπλέον, δεν χρειάζεται να γίνει καμία τροποποίηση στο λειτουργικό σύστημα επισκέπτη (guest operating system) και στις εφαρμογές της ιδεατή ή εικονικής μηχανής (virtual machine) καθώς αυτά δεν γνωρίζουν αν εκτελούνται ή όχι μέσα σε εικονικό περιβάλλον, οπότε λειτουργούν με τον ίδιο ακριβώς τρόπο που θα λειτουργούσαν μέσα σε ένα φυσικό μηχάνημα (physical machine). Αυτή η προσέγγιση έχει το πλεονέκτημα ότι επιτρέπει την πλήρη αποσύνδεση του λογισμικού από το υλικό, με αποτέλεσμα η πλήρη εικονικοποίηση (Full Virtualization) να βελτιστοποιεί τόσο την μετανάστευση (migration) των εικονικών μηχανών (virtual machines) από το ένα μηχάνημα υποδοχής (host machine) στο άλλο, όσο και τον φόρτο εργασίας μεταξύ των διαφορετικών φυσικών συστημάτων (physical systems). Επιπροσθέτως, η πλήρη εικονικοποίηση (Full Virtualization) συμβάλει στην πλήρη απομόνωση

(isolation) μεταξύ των εικονικών μηχανών (virtual machines), παρέχοντας με αυτό τον τρόπο υψηλά επίπεδα ασφαλείας **[6]**.

Η λειτουργία της τεχνική της πλήρους εικονικοποίησης (Full Virtualization) κάνει χρήση ενός συνδυασμού από εντολές δυαδικής μετάφρασης (binary translation) και εντολές που εκτελούνται απευθείας στον επεξεργαστή (processor), όπως φαίνεται στην **Εικόνα 11**. Όλες οι εφαρμογές «τρέχουν» στο επίπεδο του χρήστη και λειτουργούν σε επίπεδο δικαιωμάτων 3 (privilege level – ring 3) όπως φαίνεται και στην **Εικόνα 11**, οπότε για να πετύχουμε υψηλής απόδοσης εικονικοποίηση (high performance virtualization) ο κώδικας σε επίπεδο χρήστη εκτελείται απευθείας στον επεξεργαστή. Την ίδια στιγμή, η δυαδική μετάφραση (binary translation) χρησιμοποιείται για να μεταφράσει τον κώδικα που εκτελείται σε επίπεδο πυρήνα (kernel) με επίπεδο δικαιωμάτων 0 (privilege level – ring 0) αντικαθιστώντας τις μη-εικονικές (nonvirtualizable) εντολές με μία νέα σειρά εντολών, οι οποίες έχουν το ίδιο αποτέλεσμα στο εικονικό υλικό (virtual hardware). Για να επιτευχθεί το παραπάνω, ο hypervisor σαρώνει την μνήμη των εικονικών μηχανών (virtual machines) και «παγιδεύει» όλες τις μη-εικονικές (nonvirtualizable) εντολές πριν αυτές εκτελεστούν. Στην συνέχεια, ο hypervisor μεταφράζει δυναμικά αυτές τις εντολές σε κώδικα, τις εκτελεί και αποθηκεύει τα αποτελέσματα στην κρυφή μνήμη (cache) για μελλοντική χρήση στα δακτυλίδια (rings) που πρέπει αυτές να εκτελεστούν, πλην του δακτυλιδιού (ring) 0 **[7]**.

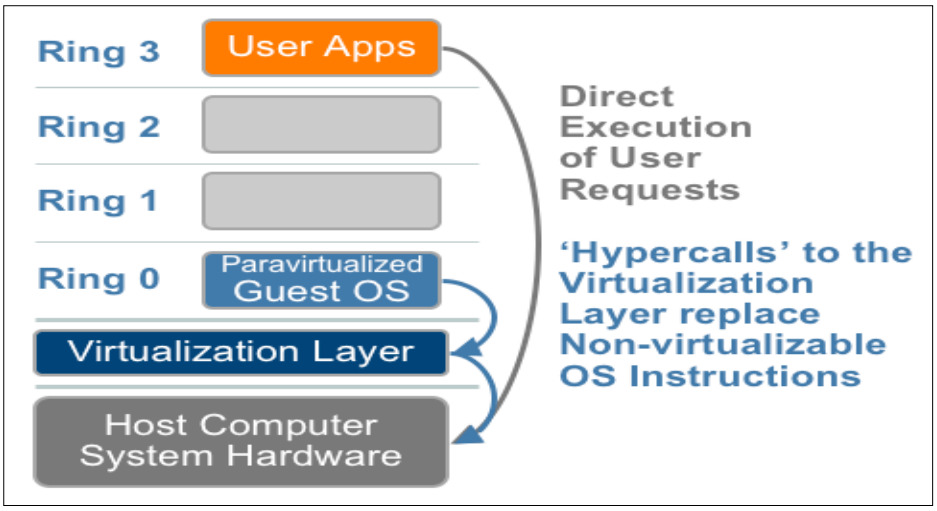


Εικόνα 11 – Πλήρης Εικονικοποίηση (Full Virtualization) [52]

2.2.5.2. Para-Εικονικοποίηση (Para-Virtualization)

Η τεχνική της Para-Εικονικοποίησης (Para-Virtualization) απαιτεί να γίνουν τροποποιήσεις στα λειτουργικά συστήματα επισκεπτών (guest operating systems) των ιδεατών ή εικονικών μηχανών (virtual machines) παρέχοντας καλύτερη απόδοση στην λειτουργία του συστήματος σε σχέση με την πλήρη εικονικοποίηση (Full Virtualization). Αυτό έχει ως αποτέλεσμα τα λειτουργικά συστήματα επισκεπτών (guest operating systems) να γνωρίζουν ότι εκτελούνται μέσα σε ένα περιβάλλον εικονικοποίησης. Ωστόσο, η τεχνική της Para-Εικονικοποίησης (Para-Virtualization) παρουσιάζει περισσότερα θέματα ασφαλείας και δεν υποστηρίζει όλα τα λειτουργικά συστήματα, λόγω των τροποποιήσεων που απαιτούνται **[6]**.

Η Para-Εικονικοποίηση (Para-Virtualization) είναι μία τεχνική εικονικοποίησης (virtualization), η οποία χρησιμοποιεί την επικοινωνία μεταξύ του hypervisor και του λειτουργικού συστήματος επισκέπτη (guest operating system) με σκοπό να βελτιώσει την απόδοση και την αποτελεσματικότητα του συστήματος. Η Para-Εικονικοποίηση (Para-Virtualization), όπως φαίνεται στην **Εικόνα 12**, τροποποιεί τον πυρήνα (kernel) του λειτουργικού συστήματος επισκέπτη (guest operating system) έτσι ώστε οι μη-εικονικές (nonvirtualizable) εντολές να αντικατασταθούν με εντολές hypercalls, οι οποίες επικοινωνούν απευθείας με τον hypervisor. Μία εντολή hypercall λειτουργεί όπως οι κλήσεις συστήματος σε περιβάλλον Linux (Linux system call) και ουσιαστικά δίνει τον έλεγχο εκτέλεσης της στον hypervisor με επίπεδο δικαιωμάτων 0 (privilege level – ring 0). Στην συνέχεια ο hypervisor εκτελεί την εντολή και επιστρέφει το αποτέλεσμα της πίσω στο λειτουργικό σύστημα επισκέπτη (guest operating system), αυτό σημαίνει ότι ο hypervisor πρέπει να παρακολουθεί συνεχώς το λειτουργικό σύστημα επισκέπτη (guest operating system) για να «παγιδεύει» τις εντολές που θα αποτύχουν **[7]**.

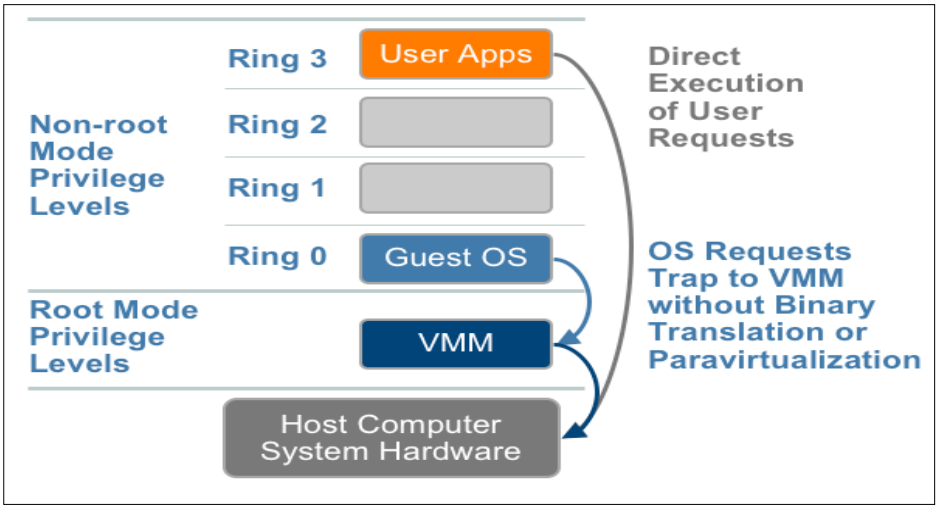


Εικόνα 12 - Para-Εικονικοποίηση (Para-Virtualization) [53]

2.2.5.3. Hardware-Assisted (Accelerated Virtualization) ή Native Εικονικοποίηση (Virtualization)

Τα σημαντικά πλεονεκτήματα που προσφέρει η εικονικοποίηση (virtualization) καθώς επίσης και η μεγάλη ζήτηση στην αγορά για λύσεις που βασίζονται στην εικονικοποίηση (virtualization) οδήγησαν τους chipset κατασκευαστές Intel και AMD στην παραγωγή επεξεργαστών που απλοποιούν την λειτουργία της εικονικοποίησης (virtualization). Έτσι λοιπόν η πρώτης γενιάς επεξεργαστές που κατασκευάστηκαν γι αυτό τον σκοπό ήταν οι Intel Virtualization Technology (VT-x) και AMD-V των εταιρειών Intel και AMD αντίστοιχα. Αυτού του είδους οι επεξεργαστές παρέχουν ένα νέο τρόπο λειτουργίας (execution mode) της ΚΜΕ (CPU), ο οποίος ονομάζεται root mode. Αυτός ο τρόπος λειτουργίας επιτρέπει στον hypervisor να «τρέχει» ένα στρώμα (layer) κάτω από τον δακτύλιο (ring) 0 και έτσι έχει τον έλεγχο του λειτουργικού συστήματος επισκέπτη (guest operating system), όπως φαίνεται στην **Εικόνα 13**. Η τεχνική της Hardware-Assisted Εικονικοποίησης (Virtualization) καταργεί την ανάγκη είτε για δυαδική μετάφραση (binary translation) ή για para-virtualization, καθώς ευαίσθητες (sensitive) ή προνομιακές (privileged) κλήσεις παγιδεύονται αυτόματα από τον hypervisor

και ταυτόχρονα δεν χρειάζεται να γίνει καμία τροποποίηση στο λειτουργικό σύστημα επισκέπτη (guest operating system) [7].



Εικόνα 13 - Hardware-Assisted (Accelerated Virtualization) or Native Εικονικοποίηση (Virtualization) [54]

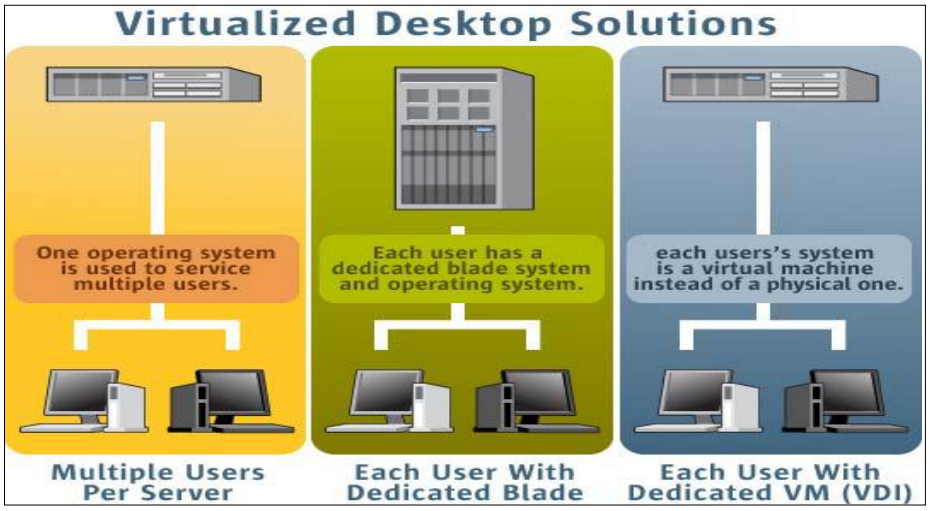
2.2.6. Άλλες Τεχνικές Εικονικοποίησης (Virtualization)

2.2.6.1. Desktop Εικονικοποίηση (Virtualization)

Η Desktop Εικονικοποίηση (Virtualization), γνωστή και ως Client Virtualization, βασίζεται στην ιδέα του διαχωρισμού της λογικής επιφάνειας εργασίας (logical desktop) από την φυσική μηχανή (physical machine) κάνοντας χρήση του μοντέλου πελάτης-εξυπηρετητής (client-server model). Σύμφωνα με αυτό το μοντέλο, η εικονική μηχανή (virtual machine) έχει εγκατασταθεί σε ένα κέντρο δεδομένων εξυπηρετητή (data center server) και είναι διαθέσιμή στον χρήστη από οπουδήποτε. Ο χρήστης αντί να αλληλεπιδρά με τον κεντρικό υπολογιστή (host computer) άμεσα, χρησιμοποιεί έναν άλλο υπολογιστή ή μια κινητή συσκευή μέσω μιας σύνδεσης δικτύου όπως ένα τοπικό δίκτυο (LAN) ή το διαδίκτυο (internet). Επιπλέον, ο κεντρικός υπολογιστής διαδραματίζει το ρόλο του εξυπηρετητή και έχει την ικανότητα να φιλοξενεί πολλαπλές εικονικές μηχανές (virtual

machines) ταυτόχρονα για πολλαπλούς χρήστες. Ο χρήστης μπορεί να είναι ένα thin-terminal ή οποιοδήποτε άλλου είδους τερματικό ακόμη και μία εφαρμογή, η οποία επιτρέπει στον χρήστη να επικοινωνεί με τον κεντρικό υπολογιστή, όπως φαίνεται στην **Εικόνα 14**. Το μοντέλο πελάτης-εξυπηρετητής (client-server model) είναι αυτό που χρησιμοποιείται κατά βάση σε περιβάλλοντα υπολογιστικού νέφους (cloud computing).

Ένα από τα πιο γνωστά είδη Desktop Εικονικοποίησης (Virtualization) είναι η Virtual Desktop Infrastructure (VDI). Η Virtual Desktop Infrastructure (VDI) καθιστά εφικτή την αποσυμφόρηση του φόρτου εργασίας ανάμεσα στους υπολογιστές και στα κέντρα δεδομένων (data center) με χρήση της τεχνικής μετανάστευσης (migration) και επιπλέον βοηθάει στην σωστή κατανομή των πόρων ενός εξυπηρετητή, μεταξύ των χρηστών **[8]**.



Εικόνα 14 - Desktop Εικονικοποίηση (Virtualization) [55]

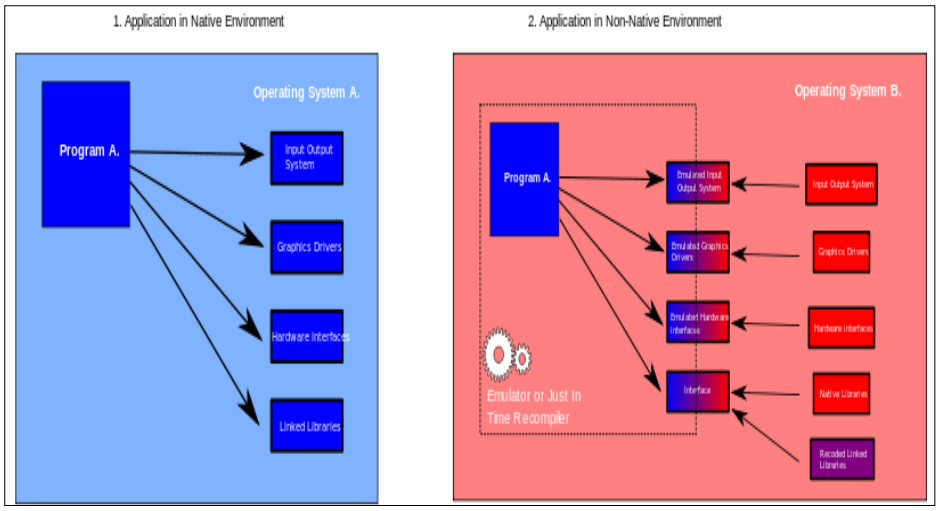
2.2.6.2. Εικονικοποίηση Εφαρμογών (Application Virtualization)

Μία νέα μορφή εικονικοποίησης (virtualization) είναι η Εικονικοποίηση Εφαρμογών (Application Virtualization), όπως φαίνεται στην **Εικόνα 15**. Η Εικονικοποίηση Εφαρμογών (Application Virtualization) είναι η πρακτική της εκτέλεσης λογισμικού από έναν απομακρυσμένο εξυπηρετητή (server), και όχι από τον υπολογιστή του χρήστη και χρησιμοποιείται για να βελτιώσει τις δυνατότητες συμβατότητας (compatibility) και φορητότητας (portability) των

εφαρμογών. Για να επιτευχθεί αύτη η δυνατότητα η εικονική εφαρμογή (virtualized application) ενθυλακώνεται (encapsulated) από ένα στρώμα εικονικοποίησης (virtualization layer), με αποτέλεσμα να εκτελείται στον υπολογιστή του χρήστη σαν να έχει εγκατασταθεί σε αυτόν. Στην ουσία αυτό το στρώμα εικονικοποίησης (virtualization layer) αντικαθιστά το περιβάλλον του χρόνου εκτέλεσης (run-time environment) που είτε εγκαθίσταται σε έναν υπολογιστή μαζί με την εφαρμογή ή υπάρχει ήδη στο σύστημα **[9]**. Στη συνέχεια, δυναμικές βιβλιοθήκες προωθούν όλες τις κλήσεις της εικονικής εφαρμογής (virtualized application) στο σύστημα αρχείων (file system) του εξυπηρετητή (server). Όταν ένα λογισμικό εκτελείται από τον εξυπηρετητή (server) με αυτό τον τρόπο, δεν γίνονται αλλαγές στο λειτουργικό σύστημα, στο σύστημα αρχείων (file system) και στο μητρώο (registry) του τοπικού υπολογιστή και επιπλέον οι υπολογιστικοί πόροι δεσμεύονται με βάση τις ανάγκες.

Μερικά από τα πλεονεκτήματα της Εικονικοποίησης Εφαρμογών (Application Virtualization) είναι:

- Εξοικονόμηση σε υλικό (hardware).
- Εξοικονόμηση σε άδειες για λογισμικό και λειτουργικά συστήματα.
- Δυνατότητα διαχείρισης υψηλού και μεταβαλλόμενου όγκου εργασίας.
- Δυνατότητα εκτέλεσης πολλαπλών εκδόσεων μίας εφαρμογής ταυτόχρονα στον ίδιο υπολογιστή.
- Ευκολία στην διαχείριση, την αναβάθμιση και την μετακίνηση των εφαρμογών.
- Βέλτιστη χρήση του διαθέσιμου υλικού (hardware).



Εικόνα 15 - Εικονικοποίηση Εφαρμογών (Application Virtualization) [56]

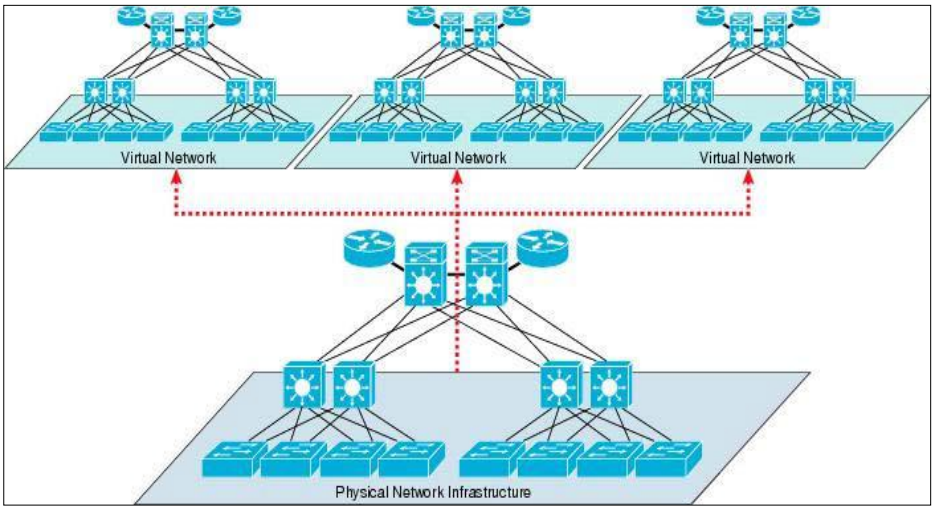
2.2.6.3. Εικονικοποίηση Δικτύου (Network Virtualization)

Η Εικονικοποίηση Δικτύου (Network Virtualization) είναι η μέθοδος συνδυασμού των διαθέσιμων πόρων σ' ένα δίκτυο χωρίζοντας το διαθέσιμο εύρος ζώνης (bandwidth) σε κανάλια (channels), κάθε ένα από τα οποία είναι ανεξάρτητο από τα άλλα και μπορεί να ανατεθεί (ή να επανατεθεί) σε έναν συγκεκριμένο εξυπηρετητή (server) ή συσκευή σε πραγματικό χρόνο, όπως απεικονίζεται στην **Εικόνα 16**. Επιπλέον, κάθε κανάλι ασφαλίζεται ανεξάρτητα και κάθε συνδρομητής έχει κοινή πρόσβαση σε όλους τους πόρους του δικτύου από έναν υπολογιστή. Αυτό επιτυγχάνεται με την βοήθεια λογισμικού και υπηρεσιών που επιτρέπουν την κοινή χρήση δικτυακών πόρων.

Έτσι, λοιπόν, για να πετύχουμε την Εικονικοποίηση του Δικτύου (Network Virtualization) πρέπει διαφορετικοί δρομολογητές μετάδοσης δεδομένων και διαφορετικές τεχνολογίες εικονικοποίησης (virtualization) να διασυνδεθούν με εικονικούς δρομολογητές. Η Εικονικοποίηση Δικτύου (Network Virtualization) έχει σαν αποτέλεσμα ένας δρομολογητής να υποστηρίζει πολλαπλούς εικονικούς δρομολογητές και κάθε εικονικός δρομολογητής να έχει την δική του ανεξάρτητη διαμόρφωση δικτύου και το δικό του ανεξάρτητο δίκτυο. Με αυτό τον τρόπο οι υπάρχουσες υποδομές μπορούν να υποστηρίξουν διαφορετικές εφαρμογές, οι οποίες να «τρέχουν»

ταυτόχρονα κάνοντας χρήση των δικών τους ανεξάρτητων δικτύων δρομολόγησης και δικαιωμάτων πρόσβασης.

Ένα εικονικό δίκτυο (virtual network) θεωρεί όλο το υλικό και το λογισμικό στο δίκτυο ως μια ενιαία συλλογή πόρων, η οποία μπορεί να προσεγγιστεί ανεξάρτητα από τα φυσικά όρια του. Με άλλα λόγια η Εικονικοποίηση Δικτύου (Network Virtualization) επιτρέπει σε κάθε εξουσιοδοτημένο χρήστη να μοιραστεί δικτυακούς πόρους από ένα μόνο υπολογιστή. Τέλος, η Εικονικοποίηση Δικτύου (Network Virtualization) βελτιστοποιεί την ταχύτητα, την αξιοπιστία, την ευελιξία, την επεκτασιμότητα, και την ασφάλεια του δικτύου.



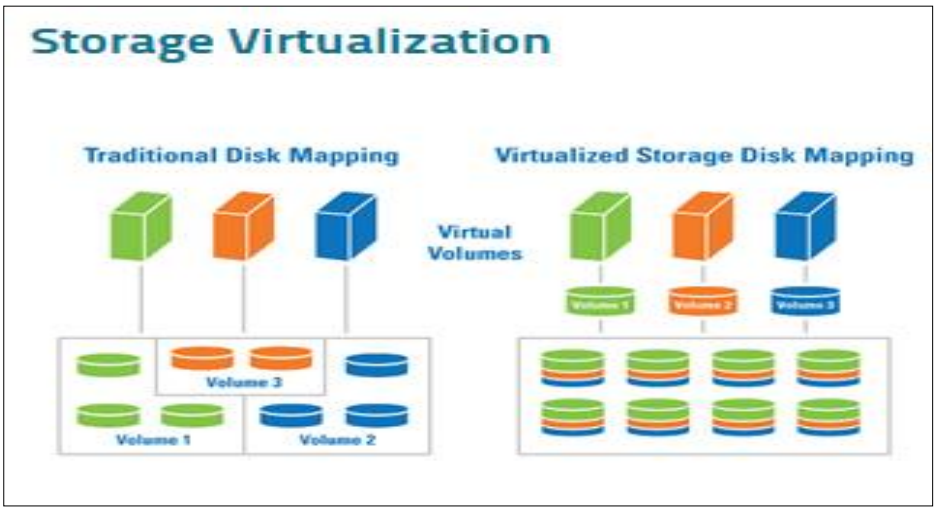
Εικόνα 16 - Εικονικοποίηση Δικτύου (Network Virtualization) [57]

2.2.6.4. Εικονικοποίηση Αποθήκευσης (Storage Virtualization)

Με τον όρο Εικονικοποίηση Αποθήκευσης (Storage Virtualization) εννοείται η λογική παρουσίαση φυσικών πολλαπλών αποθηκευτικών συσκευών, καθώς ξεχωριστές φυσικές συσκευές αποθήκευσης συνδυάζονται για να σχηματίσουν μία ενοποιημένη δεξαμενή αποθήκευσης (storage pool), η οποία παρουσιάζεται στους διακομιστές (servers) ως μία φυσική συσκευή αποθήκευσης, όπως φαίνεται στην **Εικόνα 17**. Η Εικονικοποίηση Αποθήκευσης (Storage Virtualization) είναι ουσιαστικά η πράξη της αφαίρεσης των εσωτερικών λειτουργιών των συστημάτων και υπηρεσιών αποθήκευσης

από τις εφαρμογές, τους υπολογιστές και τους δικτυακούς πόρους, με σκοπό τη δυνατότητα διαχείρισης της αποθήκευσης δεδομένων ανεξάρτητα από το δίκτυο και από τις εφαρμογές.

Η Εικονικοποίηση Αποθήκευσης (Storage Virtualization) μπορεί να βρίσκεται στο επίπεδο του κεντρικού υπολογιστή, σε συστοιχίες αποθήκευσης, ή στο δίκτυο, μέσω οπτικών μεταγωγών ή συσκευών εγκατεστημένων πάνω σε κεντρικά συστήματα αποθήκευσης (Storage Area Network (SAN)). Επιπλέον, η Εικονικοποίηση Αποθήκευσης (Storage Virtualization) παρέχει τα μέσα για τη δημιουργία υψηλού επιπέδου υπηρεσιών αποθήκευσης που κρύβουν την πολυπλοκότητα όλων των εμπλεκόμενων μερών και επιτρέπουν την αυτοματοποίηση της αποθήκευσης δεδομένων. Ο απώτερος στόχος της Εικονικοποίησης Αποθήκευσης (Storage Virtualization) είναι η απλοποίηση της διαχείρισης και αυτό μπορεί να επιτευχθεί με μια πολυεπίπεδη προσέγγιση, ενώνοντας πολλαπλά τεχνολογικά επίπεδα στο πλαίσιο της λογικής αφαίρεσης.



Εικόνα 17 - Εικονικοποίηση Αποθήκευσης (Storage Virtualization) [58]

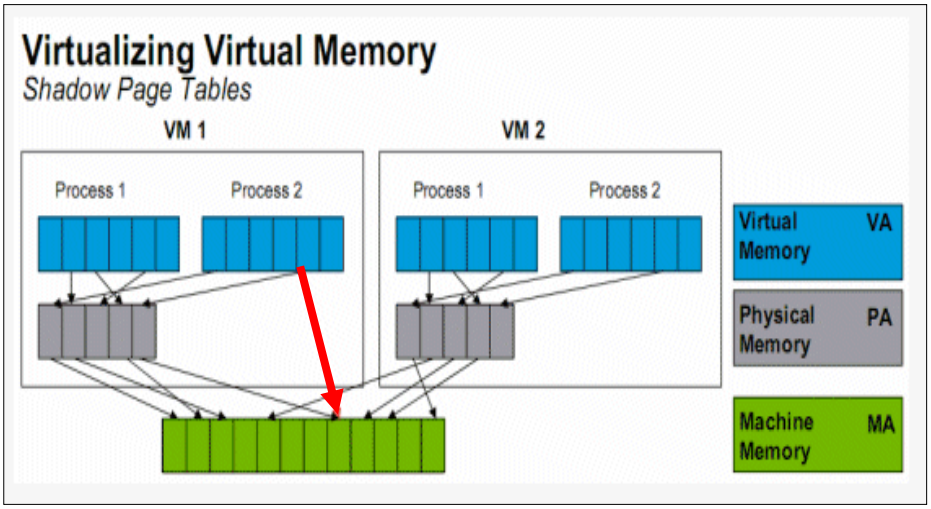
2.2.6.5. Εικονικοποίηση Μνήμης (Memory Virtualization)

Η Εικονικοποίηση Μνήμης (Memory Virtualization) είναι η μέθοδος σύμφωνα με την οποία η φυσική μνήμη του συστήματος μοιράζεται δυναμικά και κατανέμεται στις εικονικές μηχανές (virtual machines). Με αυτόν τον τρόπο, οι εφαρμογές χρησιμοποιούν έναν συνεχόμενο χώρο διευθύνσεων

(address space), ο οποίος δεν είναι απαραίτητα συνδεδεμένος με την φυσική μνήμη του συστήματος. Επιπλέον, για την βελτιστοποίηση της απόδοσης, το λειτουργικό σύστημα διατηρεί πίνακες σελίδας (page tables) στους οποίους καταγράφονται οι αντιστοιχίσεις (mapping) των εικονικών αριθμών σελίδας προς τους φυσικούς αριθμούς σελίδας και ο επεξεργαστής περιλαμβάνει μία μονάδα διαχείρισης μνήμης (Memory Management Unit (MMU)) και έναν μπάφερ (Translation Loookaside Buffer (TLB)).

Για να «τρέξουν» πολλαπλές εικονικές μηχανές (virtual machines) σε ένα υπολογιστικό σύστημα απαιτείται ένα επιπλέον στρώμα εικονικοποίησης μνήμης (memory virtualization). Αυτό το στρώμα αναλαμβάνει την εικονικοποίηση της μονάδας διαχείρισης μνήμης (Memory Management Unit (MMU)), έτσι ώστε αυτή με τη σειρά της να υποστηρίξει το λειτουργικό σύστημα επισκέπτη (guest operating system). Έτσι λοιπόν το λειτουργικό σύστημα επισκέπτη (guest operating system) ελέγχει τις αντιστοιχίσεις (mapping) των εικονικών διευθύνσεων με τις φυσικές διευθύνσεις της μνήμης του επισκέπτη, άλλα το λειτουργικό σύστημα επισκέπτη (guest operating system) δεν έχει άμεση πρόσβαση στην πραγματική φυσική μνήμη του μηχανήματος υποδοχής (host machine). Ο hypervisor είναι υπεύθυνος για να κάνει τις αντιστοιχίσεις (mapping) μεταξύ των φυσικών διευθύνσεων της μνήμης του επισκέπτη προς τις φυσικές διευθύνσεις της πραγματικής φυσικής μνήμης του μηχανήματος υποδοχής (host machine) και για να το επιτύχει αυτό χρησιμοποιεί τους κρυφούς πίνακες σελίδας (shadow page tables). Επιπροσθέτως, ο hypervisor χρησιμοποιεί τον μπάφερ (Translation Loookaside Buffer (TLB)) ώστε να κάνει και απευθείας αντιστοιχίσεις μεταξύ των εικονικών διευθύνσεων προς τις φυσικές διευθύνσεις της πραγματικής φυσικής μνήμης του μηχανήματος υποδοχής (host machine), αποφεύγοντας προς κέρδος χρόνου τα δύο επίπεδα αντιστοιχίσεων σε κάθε πρόσβαση, όπως απεικονίζεται με το κόκκινο βέλος στην **Εικόνα 18**. Τέλος, κάθε φορά που το λειτουργικό σύστημα επισκέπτη (guest operating system) αλλάζει τις αντιστοιχίσεις (mapping) μεταξύ των εικονικών διευθύνσεων προς τις φυσικές διευθύνσεις της μνήμης του επισκέπτη, ο hypervisor ενημερώνει τους κρυφούς πίνακες σελίδας (shadow page tables) ώστε να καταστεί δυνατή

τόσο η άμεση αναζήτηση όσο και η απευθείας αντιστοίχιση από τις εικονικές διευθύνσεις προς τις φυσικές διευθύνσεις της πραγματικής φυσικής μνήμης του μηχανήματος υποδοχής (host machine) **[7]**.



Εικόνα 18 - Εικονικοποίηση Μνήμης (Memory Virtualization) [59]

2.3. Ασφάλεια Εικονικοποίησης (Virtualization)

Η εικονικοποίηση (virtualization) βελτιώνει την ασφάλεια ενός συστήματος καθώς αποτελείται από λογισμικό με περισσότερες δυνατότητες σε σχέση με ένα «συμβατικό» σύστημα. Έχοντας, λοιπόν, σε λειτουργία διαφορετικά λειτουργικά συστήματα στο ίδιο φυσικό μηχάνημα ελαχιστοποιείται η ζημιά που μπορεί να προκαλέσει ένας εισβολέας καθώς τα λειτουργικά συστήματα θα έχουν διαφορετικές διαμορφώσεις και διαφορετικά τρωτά σημεία. Γενικότερα η εικονικοποίηση προσφέρει περισσότερη ευελιξία σε ένα σύστημα αφού εάν ένας χρήστης «μολυνθεί», για παράδειγμα, από «κακόβουλο» (malicious) λογισμικό τότε ένα νέο εικονικό μηχάνημα (virtual machine) μπορεί να εκκινήσει σε δευτερόλεπτα έτσι ώστε να αντικαταστήσει το «μολυσμένο» μηχάνημα του χρήστη.

Με τη βοήθεια της εικονικοποίησης (virtualization) μπορούμε να μειώσουμε τον αριθμό των εν λειτουργία εφαρμογών σε ένα μόνο μηχάνημα. Ένας φυσικός εξυπηρετητής (server) μπορεί να φιλοξενεί σε μία βάση δεδομένων ταυτόχρονα έναν εξυπηρετητή διαδικτύου (webserver) και

πολλαπλές εφαρμογές και υπηρεσίες. Μέσα όμως σε ένα περιβάλλον εικονικοποίησης μπορούμε να επιτύχουμε αποκέντρωση καθώς μία εικονική μηχανή (virtual machine) μπορεί να φιλοξενεί τον εξυπηρετητή διαδικτύου (webserver) με την βάση δεδομένων του και σε μία άλλη μπορεί να «τρέχει» μία εφαρμογή με την βάση δεδομένων της. Αυτή η αποκέντρωση εφαρμογών και υπηρεσιών οδηγεί σε καλύτερο έλεγχο και παρακολούθηση του συστήματος γιατί είναι πιο εύκολο να ελεγχθεί αν μία εικονική μηχανή (virtual machine) δεν λειτουργεί σωστά ή έχει δεχθεί επίθεση. Με αυτό τον τρόπο μειώνονται και οι πιθανότητες αποτυχίας και επίθεσης του συστήματος επειδή είναι πιο δύσκολο ένας ιός να εξαπλωθεί, ένας εισβολέας να αποσπάσει πληροφορίες και μία δυσλειτουργία (bug) σε μία εφαρμογή ή υπηρεσία δεν θέτει όλο το σύστημα εκτός λειτουργίας άλλα ένα μόνο μέρος αυτού.

Επιπλέον, στο μηχάνημα υποδοχής (host machine) είναι σε λειτουργία λιγότερος αριθμός υπηρεσιών που σημαίνει λιγότερος αριθμός υπηρεσιών με πιθανές δυσλειτουργίες (bugs) ή ευπάθειες (vulnerabilities) άρα και μικρότερη πιθανότητα εκδήλωσης επίθεσης (smaller attack surface) σε σχέση με ένα μηχάνημα το οποίο φιλοξενεί πολλαπλές εφαρμογές και υπηρεσίες. Σε ένα εικονικό σύστημα, λοιπόν, η επιφάνεια επίθεσης διαμοιράζεται μεταξύ των εικονικών μηχανών (virtual machine) περιορίζοντας με αυτό τον τρόπο το ποσοστό της ζημιάς που μπορεί να προκαλέσει ένας επιτιθέμενος.

Ωστόσο, από την άλλη πλευρά, υπάρχουν προκλήσεις μέσα σε ένα σύστημα που εφαρμόζεται η τεχνολογία της εικονικοποίησης (virtualization). Μέσα σε αυτό το πλαίσιο οι κίνδυνοι για την ασφάλεια των εικονικών πληροφοριακών συστημάτων μπορούν να ταξινομηθούν γενικά σε τρεις κατηγορίες. Σε κινδύνους που προκαλούνται από 1) την αρχιτεκτονική του συστήματος, 2) το λογισμικό του hypervisor και 3) τον τρόπο διαμόρφωσης (configuration) του συστήματος. Στο Κεφάλαιο 3 παρακάτω θα εξετάσουμε με περισσότερη λεπτομέρεια τις ευπάθειες και τις αντίστοιχες απειλές των συστημάτων υπολογιστικού νέφους (cloud computing systems) που βασίζονται στην εικονικοποίηση (virtualization).

Στην πρώτη κατηγορία εντάσσονται επιθέσεις στις εικονικές μηχανές (virtual machines), καθώς με βάση την αρχιτεκτονική λειτουργίας ενός

συστήματος εικονικοποίησης (virtualization) είναι οι πιο αδύναμοι κρίκοι άρα και πιο ευάλωτες σε επιθέσεις. Μία εικονική μηχανή (virtual machine) μπορεί να δεχθεί επίθεση είτε άμεσα ή να παραβιαστεί από έναν ιό ή «κακόβουλο» λογισμικό (malware), τα οποία μπορούν να βρουν πρόσφορο έδαφος ενεργείας καθότι η εικονική μηχανή (virtual machine) συνδέεται με διάφορες συσκευές και εκτελεί εφαρμογές και υπηρεσίες με αυξημένα δικαιώματα έχοντας το δικό της λειτουργικό σύστημα. Παρόλο που οι εικονικές μηχανές (virtual machines) είναι απομονωμένες (isolated) η μία από την άλλη για μεγαλύτερη ασφάλεια το γεγονός ότι μοιράζονται κοινούς υπολογιστικούς πόρους κάνοντας χρήση του ίδιου υλικού μπορεί να αποδειχθεί πολύ επικίνδυνο καθώς το υλικό μοιράζεται ανάμεσα στους χρήστες των εικονικών μηχανών (virtual machines), οι οποίοι δεν είναι ούτε γνωστοί ούτε αξιόπιστοι. Επιπλέον, οι εικονικές μηχανές (virtual machines) είναι μικρές σε μέγεθος με αποτέλεσμα να μπορούν να αντιγραφούν πολύ εύκολα σε μία μονάδα αφαιρούμενου δίσκου (USB) από οποιονδήποτε έχει φυσική πρόσβαση στον διακομιστή (server).

Στη δεύτερη κατηγορία εντάσσονται επιθέσεις στο λογισμικό του hypervisor, ο οποίος αποτελεί ένα μοναδικό σημείο αποτυχίας (single point of failure), που σημαίνει ότι αν ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση μπορεί να θέσει τις εικονικές μηχανές (virtual machines), που διαχειρίζονται από αυτών, σε κίνδυνο. Επιπλέον, σε υλοποιήσεις τύπου 2 hypervisor, πέραν του hypervisor και το λειτουργικό σύστημα του μηχάνημα υποδοχής (host operating system) είναι επίσης ένα μοναδικό σημείο αποτυχίας (single point of failure), πράγμα που σημαίνει ότι αν ο επιτιθέμενος καταφέρει να το θέσει σε κίνδυνο έχει σαν αποτέλεσμα να τεθούν σε κίνδυνο όλες οι εικονικές μηχανές (virtual machines) που «τρέχουν» σε αυτό.

Τέλος, στην τρίτη κατηγορία κατατάσσονται αδυναμίες διαμόρφωσης (configuration) καθώς λόγω της ευκολίας μετανάστευσης (migration), κλωνοποίησης (cloning) και αντιγραφής (copy) των εικόνων (images) των εικονικών μηχανών (virtual machines) μπορεί πολύ εύκολα να δημιουργηθεί μία νέα υποδομή. Αυτό έχει σαν αποτέλεσμα να προκύψουν αδυναμίες και

προβλήματα διαχείρισης και ελέγχου του νέου περιβάλλοντος αφού οι απαιτήσεις διαχείρισης και ελέγχου θα αυξάνονται συνεχώς.

Προκειμένου λοιπόν να περιορίσουμε, και αν είναι δυνατόν να εξαλείψουμε, αυτούς τους κινδύνους ένας οργανισμός πρέπει να υιοθετήσει ένα ασφαλές πλαίσιο λειτουργίας ώστε να διασφαλίσει την ασφάλεια των πληροφοριών (information security) και γενικά την ασφάλεια της λειτουργίας των εικονικών πληροφοριακών του συστημάτων. Μέσα σε αυτό το πλαίσιο, λοιπόν, ένας οργανισμός θα πρέπει να εγκαθιδρύσει πολιτικές και διαδικασίες, οι οποίες πρέπει να περιλαμβάνουν ένα πρόγραμμα ελέγχου (audit program) προσανατολισμένο στα εικονικά πληροφορικά του συστήματα. Οι ρόλοι και οι αρμοδιότητες των διαχειριστών του συστήματος και των χρηστών αυτού θα πρέπει να καθορίζονται και να τεκμηριώνονται με σαφήνεια. Οι μέθοδοι αυθεντικοποίησης και κρυπτογράφησης πρέπει να επιλέγονται με γνώμονα την προστασία της επικοινωνίας και των ευαίσθητων δεδομένων και επιπλέον θα πρέπει να εφαρμόζεται ξεχωριστή αυθεντικοποίηση για τις εφαρμογές των διακομιστών, των λειτουργικών συστημάτων επισκεπτών (guests operating systems), του hypervisor και του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) παρέχοντας με αυτό τον τρόπο διαφορετικά επίπεδα ασφαλείας και προστασίας.

Επιπλέον, σε ένα περιβάλλον εικονικοποίησης (virtualization) απαιτείται ισχυρή διαχείριση κλειδιών (robust key management) κρυπτογράφησης τόσο για τον έλεγχο πρόσβασης όσο και για την απόδειξη της ιδιοκτησίας (proof of ownership) δεδομένων και κλειδιών. Πολιτικές πρόσβασης βάση ρόλων (role-based access policies) πρέπει να εφαρμόζονται προκειμένου να γίνεται ο διαχωρισμός των καθηκόντων, το οποίο θα διευκολύνει την απόδειξη του ποιος έχει πρόσβαση και που (proof of governance). Επίσης, κατάλληλα μέτρα διαχείρισης δεδομένων (data governance measures) απαιτούνται για τον εντοπισμό, την παρακολούθηση και τον έλεγχο των περιπτώσεων δεδομένων τα οποία περιέχουν ευαίσθητα περιουσιακά στοιχεία και κατάλληλη κρυπτογράφηση των εικονικών μηχανών (virtual machines) προκειμένου να μειωθεί ο κίνδυνος που ελλοχεύει από την πρόσβαση του χρήστη σε φυσικούς εξυπηρετητές και χώρους αποθήκευσης, οι οποίοι περιέχουν ευαίσθητα

δεδομένα. Τέλος, οι εικονικές μηχανές (virtual machines) που δεν θα χρησιμοποιηθούν ξανά πρέπει να πληρούν τις νομικές και κανονιστικές απαιτήσεις διαγραφής τους, προκειμένου να αποτραπεί η πιθανότητα διαρροής των δεδομένων (data leakage) τους, συμπεριλαμβανομένου της καταστροφής (shredding) ή ανάκλησης (revocation) των κλειδιών κρυπτογράφησης τους **[11]**. Στο Κεφάλαιο 4 παρακάτω θα παρουσιάσουμε τα μέτρα ασφαλείας που πρέπει να υιοθετούνται από τα συστήματα υπολογιστικού νέφους (cloud computing systems) με στόχο την αποφυγή και την εξάλειψη των απειλών της εικονικοποίησης (virtualization).

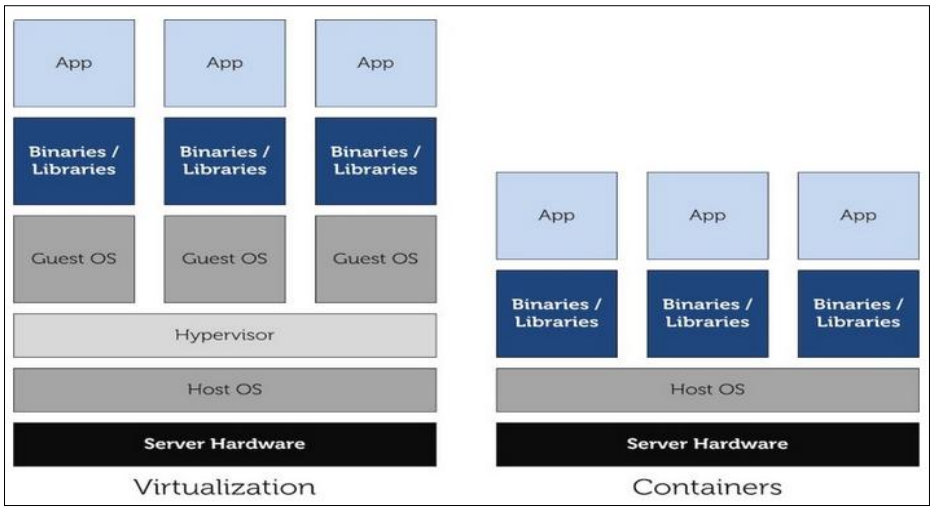
2.4. Container ή Operating System Level Virtualization

Εκτός από την τεχνική hardware virtualization ένας άλλος τρόπος υλοποίησης της τεχνολογία εικονικοποίησης (virtualization), ο οποίος παρέχει ένα απομονωμένο περιβάλλον στο εσωτερικό του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system), είναι η operating system level virtualization ή container που απεικονίζεται στην δεξιά πλευρά της **Εικόνα 19**. Κάθε container που δημιουργείται μέσα σε ένα μηχάνημα υποδοχής (host machine) είναι ένα αυτοδύναμο περιβάλλον εκτέλεσης, το οποίο μοιράζεται τον πυρήνα του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) και ταυτόχρονα είναι απομονωμένο από τα υπόλοιπα containers που λειτουργούν μέσα στο ίδιο μηχάνημα. Η πρώτη εφαρμογή αυτής της μεθόδου ήταν η τεχνολογία FreeBSD jails, επιπλέον άλλες γνωστές τεχνολογίες είναι οι Docker, Solaris Containers, OpenVZ, Linux-VServer, LXC, AIX Workload Partitions, Parallels Virtuozzo Containers και iCore Virtual Accounts **[33]**.

Σε αυτό τον τρόπο εικονικοποίησης (virtualization) τα containers χρησιμοποιούν το λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) και όχι τον hypervisor. Αντί δηλαδή της εικονικοποίησης του υλικού (hardware), με αυτή την διαδικασία εικονικοποιείται το λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) με αποτέλεσμα

ο πυρήνας του λειτουργικού συστήματος και οι πόροι του μηχανήματος να μοιράζονται μεταξύ του μηχανήματος υποδοχής (host machine) και των containers. Από τεχνικής πλευράς, ο πυρήνας του λειτουργικού συστήματος δεν γνωρίζει για την ύπαρξη των containers μέσα στο μηχάνημα υποδοχής (host machine), από την άλλη πλευρά όμως τα containers έχουν την δυνατότητα να μοιράζονται τον πυρήνα και τους πόρους με την βοήθεια των λειτουργιών namespace, chroot (change root) και cgroups (control groups). Αυτές οι λειτουργίες υπάρχουν σε πυρήνες λειτουργικών συστημάτων Linux, οπότε αυτός ο τρόπος εικονικοποίησης (virtualization) λειτουργεί πάνω στον πυρήνα του Linux και επιτρέπουν την απομόνωση των διαδικασιών, την πλήρη διαχείριση των πόρων και την ασφάλεια του περιβάλλοντος λειτουργίας των containers.

Η λειτουργία namespace συμβάλλει στην απομόνωση των διαδικασιών μεταξύ τους, κάθε φορά που απομονώνεται μία διαδικασία δημιουργείται ένα namespace. Παράλληλα η λειτουργία chroot απομονώνει κάθε διαδικασία από το σύστημα αρχείων του μηχανήματος υποδοχής (host machine). Ουσιαστικά η λειτουργία chroot απομονώνει τα namespaces από το υπόλοιπο σύστημα δημιουργώντας με αυτό τον τρόπο λογικά containers και ταυτόχρονα προστατεύει τα containers από επιθέσεις ή παρεμβολές άλλων containers που λειτουργούν μέσα στο ίδιο μηχάνημα υποδοχής (host machine). Ωστόσο, σε κάθε νέο container που δημιουργούμε πρέπει να του διαθέσουμε και πόρους, το οποίο υλοποιείται με την λειτουργία cgroups. Η λειτουργία cgroups είναι ένα χαρακτηριστικό του πυρήνα του Linux, η οποία είναι υπεύθυνη στο να καθορίζει και να απομονώνει τους πόρους, τους οποίους χρειάζεται για να λειτουργήσει μια συλλογή από διαδικασίες **[34]**.



Εικόνα 19 - Containers ή Operating System Level Virtualization [34]

2.5. Ασφάλεια Container ή Operating System Level Virtualization

Από την πλευρά της ασφάλειας, τα containers σε σχέση με ένα απλό κοινόχρηστο διακομιστή λειτουργούν καλύτερα επειδή παρέχουν καλύτερη απομόνωση. Η υλοποίηση της εικονικοποίησης (virtualization) με αυτό τον τρόπο, operating system level virtualization, είναι τόσο ασφαλής όσο και η εικονικοποίηση (virtualization) με την χρήση hypervisor, hardware virtualization, αρκεί να ακολουθηθούν σωστές πρακτικές σχεδιασμού και ανάπτυξης του περιβάλλοντος λειτουργίας των containers.

Από την άλλη πλευρά, η εικονικοποίηση (virtualization) με την χρήση containers αντιμετωπίζει προβλήματα ασφαλείας. Τα containers μοιράζονται τον πυρήνα του λειτουργικού συστήματος και ως εκ τούτου οποιαδήποτε ευπάθεια στον πυρήνα μπορεί να πλήξει την ασφάλεια όλου του συστήματος συμπεριλαμβανομένου και των containers. Επιπλέον, ο πυρήνας του λειτουργικού συστήματος παρέχει σε ένα περιβάλλον εικονικοποίησης (virtualization) πολύ περισσότερες λειτουργίες σε σχέση με τον hypervisor, με αποτέλεσμα να έχει και μεγαλύτερη επιφάνεια επίθεσης. Οι μοντέρνοι πλήρως εξοπλισμένοι πυρήνες των λειτουργικών συστημάτων εμφανίζουν πάντα

κάποιο τρωτό σημείο και επειδή τα containers εκθέτουν άμεσα τον πυρήνα σε ένα πρόγραμμα αυτό έχει σαν αποτέλεσμα την αύξηση των πιθανοτήτων παραβίασης της ασφάλειας τους **[35]**.

3

Ευπάθειες και Απειλές Εικονικοποίησης (Virtualization)

Σε αυτό το Κεφάλαιο θα εξετάσουμε τις ευπάθειες που παρουσιάζει ένα σύστημα υπολογιστικού νέφους (cloud computing system) όταν εφαρμόζεται σε αυτό η τεχνολογία της εικονικοποίησης (virtualization). Για κάθε κατηγορία ευπαθειών θα καταγράψουμε τις αντίστοιχες απειλές. Μέσα σε αυτό το πλαίσιο, λοιπόν, οι ευπάθειες και οι απειλές των συστημάτων υπολογιστικού νέφους (cloud computing systems) που βασίζονται στην εικονικοποίηση (virtualization) μπορούν να ταξινομηθούν σε τέσσερις κατηγορίες:

- Ευπάθειες και απειλές του hypervisor, όπως αυτές αναλύονται στις ενότητες 3.1., 3.2., 3.3. και 3.4. παρακάτω.
- Ευπάθειες και απειλές των εικονικών μηχανών (virtual machines), όπως αυτές αναλύονται στις ενότητες 3.5., 3.6., 3.7., 3.8. και 3.9. παρακάτω.
- Ευπάθειες και απειλές του δικτύου επικοινωνίας (network communication), όπως αυτές αναλύονται στις ενότητες 3.10. και 3.11. παρακάτω.
- Ευπάθειες και απειλές του τρόπου διαμόρφωσης (configuration) του συστήματος, όπως αυτές αναλύονται στις ενότητες 3.12. και 3.13. παρακάτω.

3.1. Απομόνωση Εικονικών Μηχανών (Isolation of Virtual Machines)

3.1.1. Ευπάθειες (Vulnerabilities)

Ο hypervisor είναι υπεύθυνος τόσο για την διαχείριση και τον έλεγχο των λειτουργικών συστημάτων επισκεπτών (guests operating systems) όσο και για την πρόσβαση αυτών στο υλικό του μηχανήματος υποδοχής (host machine) επιτρέποντας σε πολλαπλά λειτουργικά συστήματα επισκεπτών (guests operating systems) να μοιράζονται λογικά τους ίδιους φυσικούς πόρους. Ο hypervisor χωρίζει (partitions) τους πόρους του υλικού έτσι ώστε κάθε λειτουργικό σύστημα επισκέπτη (guest operating system) να έχει πρόσβαση στους δικούς του και μόνο πόρους απαγορεύοντας του να παραβιάσει είτε τους πόρους άλλου λειτουργικού συστήματος επισκέπτη (guest operating system) ή οποιαδήποτε άλλο πόρο που δεν διατίθεται προς χρήση. Με αυτό τον τρόπο πετυχαίνουμε τα λειτουργικά συστήματα επισκεπτών (guests operating systems) να λειτουργούν μεταξύ τους απομονωμένα (isolation) το ένα από το άλλο, κάτι που είναι γνωστό και ως sandboxing, αποτρέποντας τόσο την μη εξουσιοδοτημένη πρόσβαση σε πόρους όσο και την εξάπλωση «κακόβουλου» λογισμικού από το ένα λειτουργικό σύστημα επισκέπτη (guest operating system) στο άλλο.

Ωστόσο, τα λειτουργικά συστήματα επισκεπτών (guests operating systems) πολλές φορές για λόγους λειτουργικότητας δεν είναι πλήρως απομονωμένα (completely isolated) μεταξύ τους. Για παράδειγμα, πολλές λύσεις εικονικοποίησης (virtualization) παρέχουν μηχανισμούς γνωστούς ως εργαλεία επισκεπτών (guest tools) μέσω των οποίων ένα λειτουργικό σύστημα επισκέπτη (guest operating system) μπορεί να αποκτήσει πρόσβαση σε αρχεία, φακέλους και άλλους πόρους είτε του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) ή άλλου λειτουργικού συστήματος επισκέπτη (guest operating system). Αυτού του είδους οι

μηχανισμοί επικοινωνίας μπορούν ακούσια να γίνουν φορείς επίθεσης για έναν «κακόβουλο» χρήστη καθώς αυτός μπορεί είτε να μεταδώσει «κακόβουλο» λογισμικό ή να αποκτήσει πρόσβαση σε συγκεκριμένους πόρους **[12]**.

Έτσι λοιπόν μία ευπάθεια των συστημάτων υπολογιστικού νέφους (cloud computing systems) όταν εφαρμόζεται σε αυτά η τεχνολογία της εικονικοποίησης (virtualization) είναι η πρόσβαση όλων των εικονικών μηχανών στους ίδιου φυσικούς πόρους και όταν αυτό δεν γίνεται με ασφάλεια μπορεί να εξελιχθεί σε σοβαρή απειλή για το σύστημα. Επειδή, λοιπόν, γίνεται διανομή λογικών πόρων μεταξύ των χρηστών, χωρίς να γνωρίζουν οι χρήστες την πραγματική τοποθεσία των διαμοιραζόμενων πόρων, διαφορετικοί χρήστες μπορούν να δεσμεύουν τους ίδιους πόρους, όπως κοινή μνήμη, κοινό αποθηκευτικό χώρο κλπ. Ως εκ τούτου, δίνεται η δυνατότητα σε «κακόβουλους» χρήστες να αποκτήσουν πρόσβαση στα δεδομένα άλλων χρηστών μέσω της ανταλλαγής των πόρων **[13]**.

Ένας από τους κύριους στόχους του hypervisor είναι να διασφαλίζει ότι τα λειτουργικά συστήματα επισκεπτών (guests operating systems) είναι απομονωμένα (isolated), που σημαίνει ότι ένα λειτουργικό σύστημα επισκέπτη (guest operating system) δεν έχει την δυνατότητα να δεσμεύσει περισσότερους πόρους από αυτούς που του έχουν χορηγηθεί από τον hypervisor. Πολλές φορές όμως είτε λόγω εσφαλμένης διαμόρφωσης ή λόγω σχεδιαστικών λαθών του συστήματος μπορεί ένα λειτουργικό σύστημα επισκέπτη (guest operating system) να δεσμεύσει περισσότερους πόρους από αυτούς που του έχουν διατεθεί σε σχέση με τα άλλα λειτουργικά συστήματα επισκεπτών (guests operating systems) που «τρέχουν» μέσα στο ίδιο εικονικό περιβάλλον και υπό την επίβλεψη του ίδιου hypervisor. Αυτή η ευπάθεια είναι γνωστή ως VM poaching attack **[14]**.

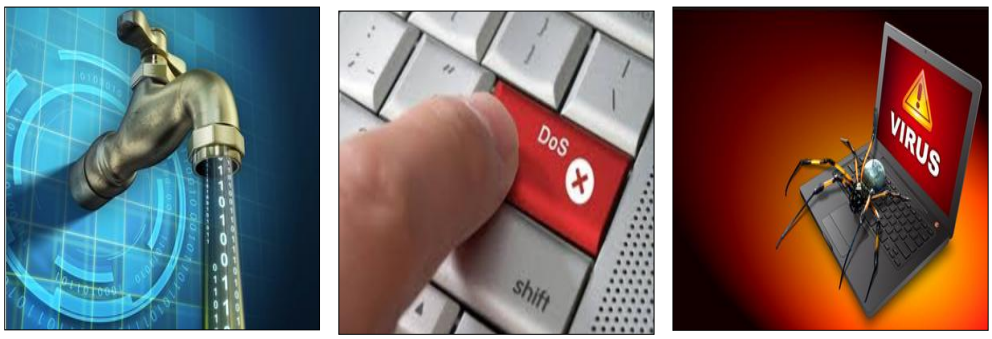
3.1.2. Απειλές (Threats)

Η απειλή που αντιμετωπίζει ένα σύστημα λόγω της κοινής πρόσβαση όλων των εικονικών μηχανών (virtual machines) στους ίδιου φυσικούς πόρους

είναι «κακόβουλοι» χρήστες να αποκτήσουν πρόσβαση στα δεδομένα άλλων χρηστών μέσω της ανταλλαγής των πόρων με αποτέλεσμα την διαρροή δεδομένων (data leakage) **[13]**. Αυτό μπορεί να έχει καταστροφικά αποτελέσματα καθώς μπορεί να προκαλέσει διαρροή μυστικών πληροφοριών, οι οποίες μπορεί να περιλαμβάνουν πληροφορίες διαχείρισης και ελέγχου της όλης υποδομής ή ακόμη και ευαίσθητα δεδομένα χρηστών του συστήματος.

Η ευπάθεια του VM poaching που είναι αποτέλεσμα είτε εσφαλμένης διαμόρφωσης ή σχεδιαστικών λαθών του συστήματος επιτρέπουν σε έναν επιτιθέμενο να δεσμεύσει περισσότερους πόρους από αυτούς που του έχουν διατεθεί. Οι απειλές που μπορούν να προκληθούν είναι:

- Άρνηση Υπηρεσίας (Denial of Service (DoS)). Μία εικονική μηχανή (virtual machine) κάνει χρήση όλων των υπολογιστικών πόρων του μηχανήματος υποδοχής (host machine), εμποδίζοντας τις άλλες εικονικές μηχανές (virtual machines) να λειτουργήσουν κανονικά.
- Διακοπή του Συστήματος (System Halt). Μια εντολή (specially crafted instruction) έχει σαν αποτέλεσμα την συντριβή (crash) είτε του hypervisor ή μίας εικονικής μηχανής (virtual machine) **[15]**.



Εικόνα 20 - Απειλές Απομόνωσης Εικονικών Μηχανών [60], [61], [62]

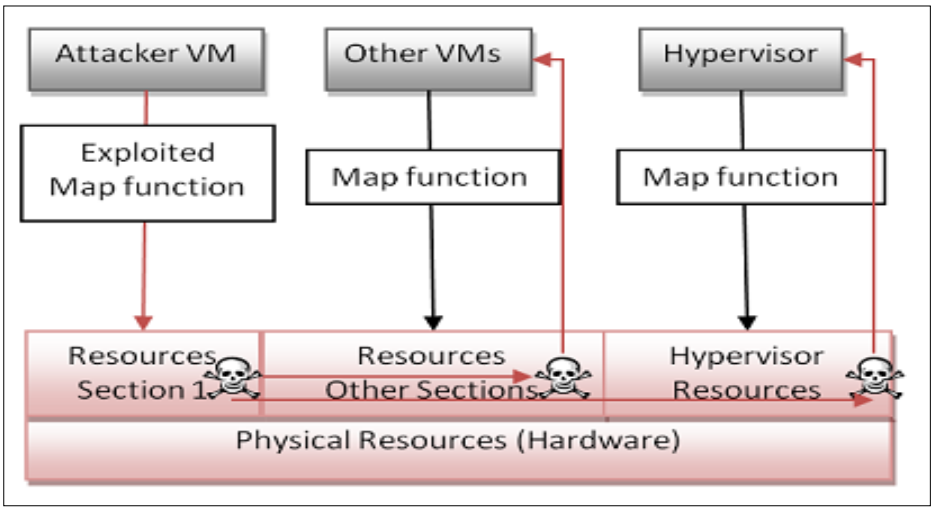
3.2. Διαφυγή Εικονικής Μηχανής (VM Escape) και Hyperjacking

3.2.1. Ευπάθειες (Vulnerabilities)

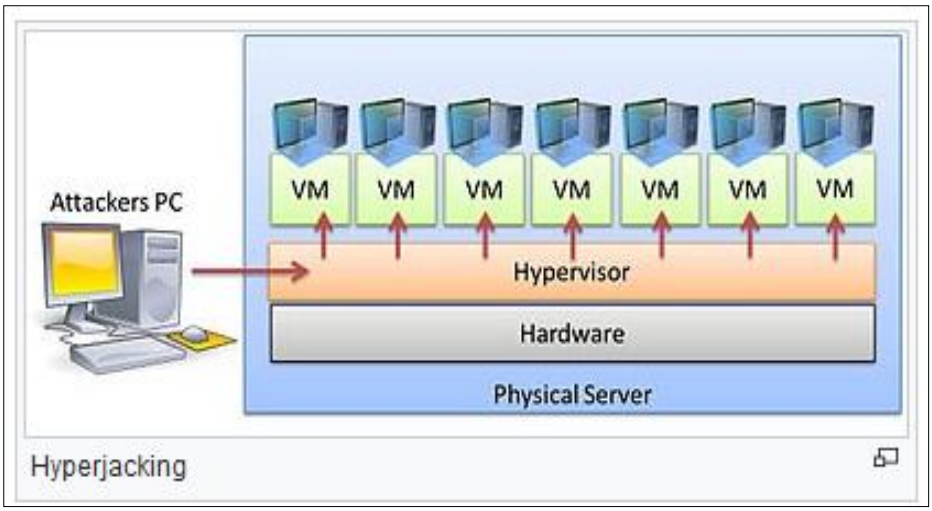
Όταν ένας επιτιθέμενος παραβιάσει το λειτουργικό σύστημα επισκέπτη (guest operating system) και αποκτήσει πρόσβαση στον hypervisor, αυτή η ευπάθεια είναι γνωστή ως διαφυγή εικονικής μηχανής (virtual machine escape) και απεικονίζεται στην **Εικόνα 21**, ενώ στην περίπτωση που έχει εγκατασταθεί λειτουργικό σύστημα στο μηχανήματος υποδοχής (host operating system) και αποκτήσει πρόσβαση σε αυτό, η ευπάθεια είναι γνωστή ως hyperjacking και απεικονίζεται στην **Εικόνα 22**. Στην περίπτωση της ευπάθειας διαφυγής εικονικής μηχανής (virtual machine escape) η επίθεση μπορεί να προκληθεί είτε από ευπάθειες του λειτουργικού συστήματος επισκέπτη (guest operating system) ή από την εκτέλεση «κακόβουλου» κώδικα, ο οποίος «τρέχει» μέσα στην εικονική μηχανή του επισκέπτη (guest virtual machine) και παρακάμπτει τους ελέγχους ασφαλείας, ή σε λάθη του hypervisor που έχουν σαν αποτέλεσμα να οδηγούν σε αδυναμίες απομόνωσης (isolation) **[12]**. Η ευπάθεια του hyperjacking είναι ένα είδος επίθεσης όπου ο επιτιθέμενος αναλαμβάνει τον έλεγχο του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) **[16]**. Για να επιτύχει τον στόχο του ο επιτιθέμενος μπορεί είτε να εισάγει έναν «κακόβουλο» hypervisor, ο οποίος αναλαμβάνει τον έλεγχο του συστήματος παρακάμπτοντας τον ήδη εγκατεστημένο hypervisor ή να αναλάβει απευθείας τον έλεγχο του εγκατεστημένου hypervisor, με απώτερο πάντα σκοπό να αποκτήσει τον έλεγχο του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system). Ο «κακόβουλος» κώδικας για την δημιουργία «κακόβουλου» hypervisor είναι γνωστός ως «VM-Based Rootkits (VMBRs)», γνωστά «VM-Based Rootkits (VMBRs)» είναι τα BLUEPILL, Vitriol, SubVir και DKSM **[17]**.

Η ασφάλεια, λοιπόν, του hypervisor είναι υψίστης σημασίας. Επομένως, πιθανές αδυναμίες που μπορεί να οδηγήσουν στην ευπάθεια τόσο του VM escape όσο και του hyperjacking, από εσωτερικούς και εξωτερικούς «κακόβουλους» επιτιθέμενους, είναι:

- Σφάλματα διαμόρφωσης του hypervisor είτε για λόγους λειτουργικότητας ή λόγω λανθασμένων ενεργειών π.χ. μη διαγραφή των υπηρεσιών που δεν χρησιμοποιούνται.
- Μη υιοθέτηση σωστών πρακτικών λειτουργίας του hypervisor.
- Μη απενεργοποίηση των συνδεδεμένων φυσικών συσκευών, των κοινόχρηστών αρχείων και φακέλων και του clipboard που δεν χρησιμοποιούνται.
- Μη διεξαγωγή άμεσου έλεγχου και διόρθωσης των ειδοποιήσεις ασφαλείας του συστήματος.
- Μη διεξαγωγή ελέγχων αυτό-ακεραιότητας (self-integrity checks) του hypervisor κατά την εκκίνηση του.
- Μη διεξαγωγή συνεχούς παρακολούθησης (monitoring) και ανάλυση των αρχείων καταγραφής (logs files) του hypervisor.
- Ανεξέλεγκτη χρήση APIs για την διαχείρισης του hypervisor και scripts οδηγεί στην περαιτέρω αύξηση της επιφάνειας επίθεσης **[11]**.



Εικόνα 21 - VM Escape [63]



Εικόνα 22 - Hyperjacking [64]

3.2.2. Απειλές (Threats)

Η απειλή που αντιμετωπίζει ένα σύστημα εάν ένας επιτιθέμενος παραβιάσει το λειτουργικό σύστημα επισκέπτη (guest operating system) αποκτώντας πρόσβαση είτε στον hypervisor ή στο λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) είναι η ανάληψη του ελέγχου όλων των εικονικών μηχανών (virtual machines) που «τρέχουν» στο συγκεκριμένο hypervisor ή στο συγκεκριμένο μηχάνημα υποδοχής (host machine) **[12]**. Επιπλέον, ο επιτιθέμενος έχει την δυνατότητα να παραβιάσει την ασφάλεια και των άλλων hypervisors με τους οποίους αλληλεπιδρά ο hypervisor, τον οποίο έχει ήδη παραβιάσει **[11]**. Η ζημιά που μπορεί να προκληθεί σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) όταν εφαρμόζεται σε αυτό η τεχνολογία της εικονικοποίησης (virtualization), από τις ευπάθειες του VM escape και hyperjacking είναι πολύ μεγάλη.

3.3. Μη Εξουσιοδοτημένη Πρόσβαση στον Hypervisor ή VMM

3.3.1. Ευπάθειες (Vulnerabilities)

Ο hypervisor είναι ευάλωτος σε άμεσες επιθέσεις και δημιουργεί μία νέα επιφάνεια επίθεσης, η οποία δεν συναντάται στα «παραδοσιακά» πληροφοριακά συστήματα. Μέσα σε αυτό το πλαίσιο και αναλόγως των απαιτήσεων ασφαλείας ενός συστήματος μπορεί τόσο η προεπιλεγμένη διαμόρφωση του hypervisor να μην ενδείκνυται και να απαιτούνται επιπλέον παραμετροποιήσεις, όσο και ο έλεγχος πρόσβασης των διαχειριστών στον hypervisor, ιδιαίτερα αν αυτός πραγματοποιείται εξ αποστάσεως, να μην είναι επαρκής για προστασία από επιθέσεις «κακόβουλων» χρηστών. Την ίδια στιγμή, το λογισμικό διαχείρισης του hypervisor, το οποίο χρησιμοποιείται για τον έλεγχο και την διαχείριση του, είναι ένας επιπλέον ελκυστικός στόχος επιθέσεων «κακόβουλων» χρηστών. Άρα, λοιπόν, τόσο ο hypervisor όσο και το λογισμικό διαχείρισης αυτού είναι ευάλωτα σε επιθέσεις «κακόβουλων» χρηστών. Επομένως, ευπάθειες του hypervisor και του λογισμικού διαχείρισης αυτού είναι:

- Μη περιορισμός πρόσβασης στο στρώμα εικονικοποίησης, όπως π.χ. μη δημιουργία κανόνων τείχους προστασίας (firewall) για περιορισμό στην χρήση της κονσόλας διαχείρισης του hypervisor.
- Μη χρήση τεχνικών αυθεντικοποίησης για περιορισμό πρόσβασης.
- Μη δυνατότητα υποστήριξη από τον hypervisor ελέγχου πρόσβασης βάση ρόλων (role-based access control) για τον διαχωρισμό των αρμοδιοτήτων των διαχειριστών.
- Μη ύπαρξη εμπορικών και μη εργαλείων (third-party tools), τα οποία μπορούν να υποστηρίξουν αυστηρούς ελέγχους ασφαλείας.
- Μη προστασία των APIs / CLIs διαχείρισης του hypervisor.

- Μη ύπαρξη ξεχωριστού δικτύου διαχείρισης (management LAN), το οποίο θα διαχειρίζεται την πρόσβαση στον hypervisor.
- Μη απενεργοποίηση της απομακρυσμένης διαχείρισης του hypervisor.
- Έλλειψη διαδικασιών σε διαχειριστικές αλλαγές και έκθεση των διεπαφών (interfaces) των διαχειριστών σε λάθη διαμόρφωσης του δικτύου (network configuration errors) **[11]**.

3.3.2. Απειλές (Threats)

Αν η διαχείριση και ο έλεγχος του hypervisor δεν ακολουθούν κανόνες ασφαλείας, οι οποίοι να θεραπεύουν όλες τις ευπάθειες που αναλύθηκαν στην προηγούμενη ενότητα τότε ο hypervisor κινδυνεύει από την απειλή της μη εξουσιοδοτημένης πρόσβασης (unauthorized access). Αυτό σημαίνει ότι ένας «κακόβουλος» χρήστης μπορεί εκμεταλλευόμενος μία ευπάθεια να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον hypervisor. Γι᾽ αυτό κρίνεται απαραίτητος ο έλεγχος ασφαλούς πρόσβασης στον hypervisor.

Εικόνα 23 - Μη Εξουσιοδοτημένη Πρόσβαση [65]

3.4. Εξάντληση Πόρων (Resource Exhaustion)

3.4.1. Ευπάθειες (Vulnerabilities)

Μέσα σε ένα περιβάλλον εικονικοποίησης (virtualization), λογισμικό που χρησιμοποιεί συγκεκριμένους πόρους του μηχανήματος υποδοχής (host machine) μπορεί να τους εξαντλήσει και ως εκ τούτου να επηρεάσει την διαθεσιμότητα των εικονικών μηχανών (virtual machines). Αυτή η κατάσταση δημιουργείτε λόγω της εξάντλησης των διαμοιραζόμενων φυσικών πόρων όταν πολλαπλές εικονικές μηχανές (virtual machines) κάνουν χρήση με την ίδια ένταση, των ίδιων πόρων, την ίδια χρονική στιγμή.

Επιπλέον, η κατάσταση αυτή έχει σαν αποτέλεσμα την επιβάρυνση και του ίδιου του διακομιστή που παρέχει τους προς χρήση πόρους καθώς η ταυτόχρονη χρήση του δίσκου είτε για ενημερώσεις λογισμικού ή για ταυτόχρονη επανεκκίνηση των εικονικών μηχανών (virtual machines) ή για ταυτόχρονη λειτουργία ανίχνευσης ιών από πολλαπλές εικονικές μηχανές (virtual machines), μπορεί να δημιουργήσει μεγάλη υπερφόρτωση στον διακομιστή με αποτέλεσμα την μείωση της απόδοσης του. Άρα, η εξάντληση των φυσικών πόρων λόγω ταυτόχρονης χρήσης τους από πολλαπλές εικονικές μηχανές (virtual machines) είναι μία ευπάθεια που χαρακτηρίζει τον hypervisor καθώς αυτός έχει την ευθύνη του ελέγχου, του τρόπου λειτουργίας και της διαχείρισης των πόρων και των εικονικών μηχανών (virtual machines) **[11]**, **[18]**.

3.4.2. Απειλές (Threats)

Για να αποφευχθεί η εξάντληση των φυσικών πόρων όταν πολλαπλές εικονικές μηχανές (virtual machines) κάνουν χρήση αυτών με την ίδια ένταση, έχουν αναπτυχθεί εργαλεία λογισμικού που είτε εφαρμόζουν αυτές τις αλλαγές

ανά ομάδες και όχι ταυτόχρονα ή προσθέτουν ένα στοιχείο τυχαίου χρόνου για το πότε οι αλλαγές θα πρέπει να ξεκινήσουν να εφαρμόζονται. Ωστόσο, από την άλλη μεριά, μία τέτοια αντιμετώπιση της συγκεκριμένης ευπάθεια μπορεί να σημαίνει ότι ένα μέρος των εικονικών μηχανών (virtual machines) θα παραμείνει χωρίς την εφαρμογή, παραδείγματος χάριν των ενημερώσεων διόρθωσης (patches) για μεγάλο χρονικό διάστημα, γεγονός που τις καθιστά ευάλωτες σε επιθέσεις. Επομένως, η απειλή που αντιμετωπίζει ένα σύστημα από την εξάντληση των πόρων είναι άρνησης υπηρεσίας (Denial of Service (DoS)), αφού ένας επιτιθέμενος θα μπορούσε σκόπιμα να χρησιμοποιήσει τους εναπομείναντες λιγοστούς πόρους για να πετύχει επίθεση άρνησης υπηρεσίας (Denial of Service (DoS)) του τοπικού διακομιστή **[18]**.

Εικόνα 24 - Denial of Service (DoS) [66]

3.5. Αδρανής (Dormant) ή Εκτός Λειτουργίας (Offline) Εικονικές Μηχανές (Virtual Machines)

3.5.1. Ευπάθειες (Vulnerabilities)

Η δυναμική φύση των εικονικών μηχανών (virtual machines) έχει σαν αποτέλεσμα να μπορούν αυτές να περνούν από την μία κατάσταση λειτουργίας, ενεργή (active - running), αδρανής (dormant - suspended) και εκτός λειτουργίας (offline - shut down), στην άλλη πολύ εύκολα και γρήγορα. Επιπλέον, οι διαχειριστές του συστήματος, πολλές φορές για λόγους απλότητας και ταχύτητας, όταν μία εικονική μηχανή (virtual machine) δεν λειτουργεί σωστά προτιμούν να την επαναφέρουν σε προηγούμενη κατάσταση καλής λειτουργίας αντί να εγκαταστήσουν μία νέα από την αρχή. Αυτή η εναλλαγή σε καταστάσεις λειτουργίας είναι αναγκαία για πολλούς λόγους, είτε γιατί τα περιβάλλοντα εικονικοποίησης (virtualization) αλλάζουν και εξελίσσονται πολύ γρήγορα ή για ανάγκες προγραμματισμένης συντήρησης ή για αποκατάσταση εικονικών μηχανών που έχουν καταστραφεί (disaster recovery) ή για παροχή περισσοτέρων υπολογιστικών πόρων.

Ωστόσο, αδρανείς (dormant - suspended), εκτός λειτουργίας (offline - shut down) και εικονικές μηχανές (virtual machines) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας μπορεί να απέχουν πάρα πολύ από την τρέχουσα κατάσταση ασφαλείας με αποτέλεσμα να είναι ευάλωτες σε μεγάλο αριθμό ευπαθειών παραβίασης της ασφάλειας τους. Επομένως, αν μία εικονική μηχανή (virtual machine) δεν είναι ενεργή κατά την διάρκεια των ενημερώσεων λογισμικού (software updates), όταν αυτή τεθεί σε κατάσταση λειτουργίας θα είναι απροστάτευτη (out-of-date) και ευάλωτη σε επιθέσεις «κακόβουλων» χρηστών. Από τα παραπάνω καταλαβαίνουμε ότι η μη έγκαιρη ενημέρωση του λογισμικού των εικονικών μηχανών (virtual machines) με τις πιο πρόσφατές ενημερώσεις (updates) και διορθώσεις (patches) είναι μία σοβαρή ευπάθεια μέσα σε ένα περιβάλλον εικονικοποίησης (virtualization), η

οποία προέρχεται από την απουσία κατευθυντήριων γραμμών σχετικά με τον τρόπο χειρισμού αδρανών (dormant), εκτός λειτουργίας (offline) και εικονικών μηχανών (virtual machines) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας τους **[11]**, **[27]**.

Εικόνα 25 - Out of Date [67]

3.5.2. Απειλές (Threats)

Οι αδρανής (dormant), οι εκτός λειτουργίας (offline) και οι εικονικές μηχανές (virtual machines) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας, λόγω έλλειψης των πιο πρόσφατων ενημερώσεων (updates) και διορθώσεων (patches), όταν αυτές τεθούν σε κατάσταση λειτουργίας ενεργή (active) είναι εκτεθειμένες σε ευπάθειες παραβίασης της ασφάλειας τους, οι οποίες μπορούν να προκαλέσουν σοβαρά κενά ασφαλείας (security loopholes) στο περιβάλλον εικονικοποίησης. Οι χρήστες, λοιπόν, που κάνουν χρήση αυτών των εικονικών μηχανών (virtual machines) αντιμετωπίζουν την απειλή της κλοπής των δεδομένων τους (data theft) **[11]**.

Εικόνα 26 - Κλοπή Δεδομένων (Data Theft) [68]

3.6. Προ-Ρυθμισμένες (Pre-Configured) Εικονικές Μηχανές (Virtual Machines)

3.6.1. Ευπάθειες (Vulnerabilities)

Οι προ-ρυθμισμένες (pre-configured) εικονικές μηχανές (virtual machines), γνωστές και ως golden image, είναι πρότυπα (templates) βάση των οποίων δημιουργούνται νέες εικονικές μηχανές, οι οποίες είναι κλώνοι των αρχικών. Η τεχνική αυτή εφαρμόζεται σε περιβάλλοντα εικονικοποίησης (virtualization) προς εξοικονόμηση χρόνου καθώς εξαλείφεται η ανάγκη για εφαρμογή επαναλαμβανόμενων ρυθμίσεων σε κάθε νέα εικονική μηχανή (virtual machine) που δημιουργείται. Ωστόσο, οι προ-ρυθμισμένες (pre-configured) εικονικές μηχανές (virtual machines), οι οποίες είναι αποθηκευμένες σε μορφή αρχείων μέσα στην πλατφόρμα της εικονικοποίησης (virtualization), είναι εκτεθειμένες σε επιθέσεις «κακόβουλων» χρηστών, όπως μη εξουσιοδοτημένες αλλαγές στο υλικό και εισαγωγή «κακόβουλου» λογισμικού. Επομένως, η έλλειψη διασφάλισης της ακεραιότητας των προ-ρυθμισμένων (pre-configured) εικονικών μηχανών (virtual machines) είναι

άλλη μία ευπάθεια που καλούνται να αντιμετωπίσουν τα περιβάλλοντα εικονικοποίησης (virtualization) **[11]**.

3.6.2. Απειλές (Threats)

Αν ένας επιτιθέμενος καταφέρει να παραβιάσει την ασφάλεια των προ-ρυθμισμένων (pre-configured) εικονικών μηχανών (virtual machines) αυτό θα έχει σαν αποτέλεσμα η πλατφόρμα εικονικοποίησης (virtualization) να αντιμετωπίσει την απειλή της απώλειας της ακεραιότητας της (loss of integrity) **[11]**.

Εικόνα 27 - Απώλεια Ακεραιότητας (Loss of Integrity) [69]

3.7. Ευαίσθητα Δεδομένα Μέσα στις Εικονικές Μηχανές (Virtual Machines)

3.7.1. Ευπάθειες (Vulnerabilities)

Οι εικονικές μηχανές (virtual machines) περιέχουν ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης (passwords), προσωπικά δεδομένα (personal

data), bash profiles, bash history files, κλειδιά κρυπτογράφησης (encryption keys) και license keys, τα οποία είναι αποθηκευμένα και μέσα στις αντίστοιχες από αυτές εικόνες (images) και στιγμιότυπα (snapshots). Τα ευαίσθητα δεδομένα, λοιπόν, μέσα σε περιβάλλοντα εικονικοποίησης (virtualization) αντιμετωπίζουν περισσότερες ευπάθειες καθώς είναι ευκολότερο να μετακινηθούν από ότι μέσα σε ένα περιβάλλον φυσικής υποδομής. Αυτό σημαίνει ότι αντίγραφα εικόνων (images) και στιγμιότυπων (snapshots) μπορούν να μετακινηθούν εύκολα και γρήγορα από ένα κέντρο δεδομένων (data center) είτε με ένα αφαιρούμενο δίσκο ή μέσω της κονσόλας του hypervisor και να εγκατασταθούν οπουδήποτε. Επιπλέον, τα στιγμιότυπα (snapshots) θέτουν τα ευαίσθητα δεδομένα σε ακόμα μεγαλύτερο κίνδυνο επειδή περιέχουν τα περιεχόμενα της μνήμης την στιγμή που ελήφθη το στιγμιότυπο (snapshot). Πέραν της ευκολίας μετακίνησης μια ακόμη σοβαρή ευπάθεια είναι αν έχουν παραμείνει εναπομείναντα δεδομένα στην προηγούμενη θέση τους, τα οποία μπορούν να εκτεθούν σε κίνδυνο.

Οι ευπάθειες που αντιμετωπίζουν τα αποθηκευμένα ευαίσθητα δεδομένα μέσα στις εικονικές μηχανές (virtual machines) είναι:

- Έλλειψη εφαρμογής πολιτικών και διαδικασιών αντιμετώπισης των εικόνων (images) και των στιγμιότυπων (snapshots) με βάση τα ευαίσθητα δεδομένα που περιέχουν.
- Έλλειψη πολιτικών και διαδικασιών περιορισμού της αποθήκευσης των εικόνων (images) και των στιγμιότυπων (snapshots) των εικονικών μηχανών (virtual machines), οι οποίες περιλαμβάνουν:
  - ✓ Έλλειψη διαδικασιών διαχείρισης των εικόνων (images) αναφορικά με τον τρόπο δημιουργίας, ασφαλείας, διανομής, αποθήκευσης, χρήσης, θέσεως τους εκτός ενεργείας και καταστροφής τους.
  - ✓ Έλλειψη παρακολούθησης και ελέγχου των αποθηκευμένων εικόνων (images) και στιγμιότυπων (snapshots), συμπεριλαμβανομένου των δραστηριοτήτων σύνδεσης σε αυτές **[11]**.

Εικόνα 28 - Ευαίσθητα Δεδομένα [70]

3.7.2. Απειλές (Threats)

Παρόλο που οι εικόνες (images) και τα στιγμιότυπα (snapshots) παρέχουν την δυνατότητα της γρήγορης και αποτελεσματικής ανάπτυξης και αποκατάστασης εικονικών μηχανών (virtual machines) σε πολλούς φυσικούς εξυπηρετητές, ταυτόχρονα εγκυμονεί και ο κίνδυνος της ασφάλειας των ευαίσθητων δεδομένων που περιέχουν οι εικονικές μηχανές (virtual machines). Μέσα σε ένα περιβάλλον εικονικοποίησης (virtualization) δεν είναι εύκολο να εξασφαλίσουμε την ασφάλεια των ευαίσθητων δεδομένων από επιθέσεις μη εξουσιοδοτημένης πρόσβασης «κακόβουλων» χρηστών. Η απειλεί που αντιμετωπίζει ένα περιβάλλον εικονικοποίησης (virtualization) είναι «κακόβουλοι» χρήστες να αποκτήσουν πρόσβαση με χρήση «κακόβουλου» λογισμικού σε εικόνες (images) και στιγμιότυπα (snapshots) εικονικών μηχανών (virtual machines) με αποτέλεσμα να θέσουν σε κίνδυνο την ασφάλεια τους αποσπώντας τα ευαίσθητα δεδομένα που αυτές περιέχουν (sensitive data theft) **[11]**.

Εικόνα 29 - Ευαίσθητα Δεδομένα [71]

3.8. Μικτό Επίπεδο Εμπιστοσύνης Εικονικών Μηχανών (Virtual Machines)

3.8.1. Ευπάθειες (Vulnerabilities)

Εικονικές μηχανές (virtual machines) στις οποίες είναι αποθηκευμένα ευαίσθητα δεδομένα μπορεί να βρίσκονται μέσα στο ίδιο μηχάνημα υποδοχής (host machine) μαζί με άλλες στις οποίες είναι αποθηκευμένα λιγότερο κρίσιμα δεδομένα. Αυτό έχει σαν αποτέλεσμα την δημιουργία ενός μικτού επιπέδου εμπιστοσύνης εικονικών μηχανών (virtual machines). Ωστόσο, οι οργανισμοί προσπαθούν για λόγους ασφαλείας να διαχωρίσουν τις εικονικές μηχανές των διαφορετικών επιπέδων εμπιστοσύνης σε ξεχωριστά μηχανήματα υποδοχής (host machines), αλλά πολλές φορές αυτός ο διαχωρισμός μπορεί να λειτουργεί εναντίον της αποτελεσματικής χρήσης των πόρων με αποτέλεσμα να είναι εναντίον του σκοπού για τον οποίο υπάρχουν τα περιβάλλοντα εικονικοποίησης (virtualization). Μέσα σε αυτό το πλαίσιο, λοιπόν, ένας οργανισμός πρέπει να εξασφαλίσει ότι οι ευαίσθητες πληροφορίες του

προστατεύονται και παράλληλα ότι εκμεταλλεύεται τα οφέλη που προσφέρει η εφαρμογή της εικονικοποίησης (virtualization) **[19]**.

Ευπάθειες που μπορεί να οδηγήσουν σε ένα περιβάλλον μικτού επιπέδου εμπιστοσύνης είναι:

- Εικονικές μηχανές (virtual machines) από διαφορετικά επίπεδα εμπιστοσύνης φιλοξενούνται ή μεταναστεύουν (migrated) στον ίδιο φυσικό εξυπηρετητή (physical server).
- Μη διαχωρισμός σε διαφορετικά επίπεδα εμπιστοσύνης των φυσικών και λογικών δικτύων των εικονικών μηχανών (virtual machines).
- Μη ανάπτυξη φυσικών και εικονικών τείχων προστασίας (firewalls) για απομόνωση ομάδων εικονικών μηχανών (virtual machines) ανάλογα με την ομάδα εργασίας που αυτές ανήκουν μέσα στο μηχάνημα υποδοχής (host machine).
- Μη ύπαρξη κανόνων διαχωρισμού των καθηκόντων των διαχειριστών προκειμένου να αποτραπούν μη εξουσιοδοτημένες αλλαγές ή τυχαίες λανθασμένες παραμετροποιήσεις **[11]**.

3.8.2. Απειλές (Threats)

Οι οργανισμοί, όπως αναφέρθηκε και προηγουμένως, προσπαθούν για λόγους ασφαλείας να διαχωρίσουν τις εικονικές μηχανές (virtual machines) των διαφορετικών επιπέδων εμπιστοσύνης σε ξεχωριστά μηχανήματα υποδοχής (host machines). Ωστόσο, αυτή η προσπάθεια δεν μπορεί να είναι αποτελεσματική αν δεν υπάρχει αποτελεσματική εφαρμογή των συστημάτων, αποτελεσματική κατηγοριοποίησης των δεδομένων και εφαρμογή κατάλληλων ελέγχων διαχείρισης, ασφαλείας και δικτύου. Έτσι εικονικές μηχανές (virtual machines) με χαμηλότερο επίπεδο εμπιστοσύνης θα έχουν πιο ελαστικούς ελέγχους ασφαλείας σε σχέση με τις εικονικές μηχανές (virtual machines) με υψηλότερο επίπεδο εμπιστοσύνης. Αυτό έχει σαν αποτέλεσμα να είναι πιο εύκολο να παραβιαστεί η ασφάλεια των εικονικών μηχανών (virtual machines) χαμηλότερου επιπέδου εμπιστοσύνης και επειδή υπάρχουν μέσα στο ίδιο

μηχάνημα υποδοχής (host machine) με εικονικές μηχανές (virtual machines) υψηλότερου επιπέδου εμπιστοσύνης εκθέτουν και αυτές σε μεγαλύτερο κίνδυνο. Εν κατακλείδι, η απειλή που αντιμετωπίζει ένα σύστημα από την φιλοξενία εικονικών μηχανών (virtual machines) διαφορετικών επιπέδων εμπιστοσύνης μέσα στο ίδιο μηχάνημα υποδοχής (host machine) είναι ότι μειώνει την συνολική ασφάλεια του συστήματος σε εκείνη που ισχύει για τα λιγότερο προστατευμένα στοιχεία του δηλαδή για τις εικονικές μηχανές (virtual machines) χαμηλότερου επιπέδου εμπιστοσύνης.

Εικόνα 30 – Μικτό Επίπεδο Εμπιστοσύνης [72]

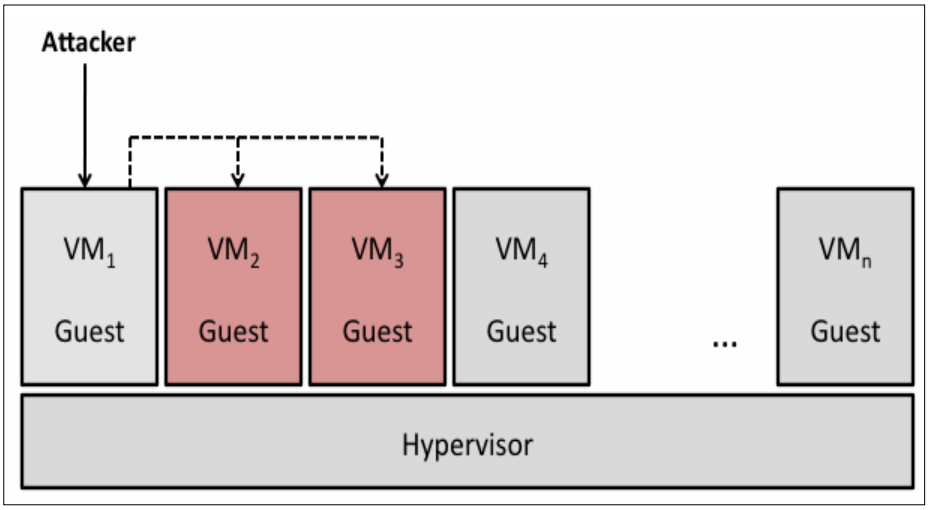
3.9. Πέρασμα από την μία Εικονική Μηχανή στην Άλλη (VM Hopping)

3.9.1. Ευπάθειες (Vulnerabilities)

Όταν πολλαπλές εικονικές μηχανές (virtual machines) «τρέχουν» στο ίδιο μηχάνημα υποδοχής (host machine), τότε ένας «κακόβουλος» επιτιθέμενος, όπως ένας απομακρυσμένος μη έμπιστος χρήστης μιας εικονικής μηχανής (virtual machine) μπορεί να πάρει τον έλεγχο μιας άλλης εικονικής μηχανής (virtual machine). Αυτή η επίθεση μεταπήδησης ενός «κακόβουλου»

χρήστη από την μία εικονική μηχανή (virtual machine) στην άλλη ονομάζεται VM Hopping. Κάθε εικονική μηχανή (virtual machine), λοιπόν, που «τρέχει» μέσα σε ένα μηχάνημα υποδοχής (virtual machine) μπορεί να γίνει στόχος επίθεσης VM Hopping **[20]**.

Η ύπαρξη μη αξιόπιστων εικονικών μηχανών (virtual machines) μέσα σε ένα περιβάλλον εικονικοποίησης (virtualization), οι οποίες μπορούν να εκτοξεύσουν μία επίθεση VM Hopping, είναι μία σοβαρή ευπάθεια που καλούνται να αντιμετωπίσουν τα συστήματα υπολογιστικού νέφους (cloud computing systems). Η ευπάθεια είναι αποτέλεσμα τόσο της λειτουργίας όλων των εικονικών μηχανών (virtual machines) μέσα στο ίδιο μηχάνημα υποδοχής (host machine) και υπό την επίβλεψη του ίδιου hypervisor όσο και επειδή ο πάροχος των υπηρεσιών υπολογιστικού νέφους (cloud provider) έχει υλοποιήσει κάποιο επίπεδο εμπιστοσύνης μεταξύ των εικονικών μηχανών (virtual machines) για το οποίο οι χρήστες δεν είναι ενημερωμένοι. Η μη αξιόπιστη εικονική μηχανή (virtual machine) θα προσπαθήσει να βρει ευπάθειες του επιπέδου εμπιστοσύνης, να τις εκμεταλλευτεί με σκοπό να διεξάγει μία επίθεση VM Hopping και να πάρει τον έλεγχο μίας άλλης εικονικής μηχανής (virtual machine) **[21]**.



Εικόνα 31 - VM Hopping [73]

3.9.2. Απειλές (Threats)

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν λάθη λογισμικού, ιούς (viruses), σκουλήκια (worms) και μη ενημερωμένα (unpatches) λειτουργικά συστήματα εκτοξεύοντας zero day attacks και να πάρουν τον έλεγχο του λειτουργικού συστήματος μιας άλλης εικονικής μηχανής (virtual machine) **[22]**. Η απειλή που αντιμετωπίζει ένα σύστημα υπολογιστικού νέφους (cloud computing system) όταν ένας επιτιθέμενος εκμεταλλευτεί την ευπάθεια του VM Hopping είναι ότι με αυτό τον τρόπο ο «κακόβουλος» χρήστης έχει την δυνατότητα να παρακολουθεί την χρήση των πόρων, να τροποποιεί τις ρυθμίσεις, να διαγράφει δεδομένα και να προκαλεί θέματα εμπιστευτικότητας της εικονικής μηχανής (virtual machine) που έχει θέσει υπό τον έλεγχο του. Επιπλέον, ο «κακόβουλος» χρήστης μπορεί να προκαλέσει άρνηση υπηρεσίας (Denial of Service (DoS)), αφού μπορεί να θέσει τους πόρους και τις υπηρεσίες μίας εικονικής μηχανής (virtual machine) μη διαθέσιμους στους χρήστες της **[20]**.

Εικόνα 32 - VM Hopping [74]

3.10. Address Resolution Protocol (ARP) Spoofing Attack

3.10.1. Ευπάθειες (Vulnerabilities)

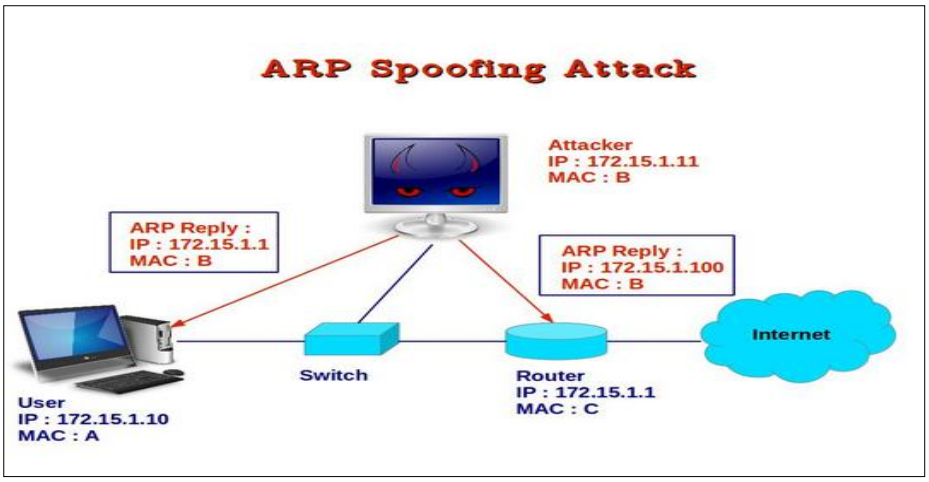
Σε ένα περιβάλλον εικονικοποίησης (virtualization) ευπάθειες παρουσιάζονται και στο δίκτυο επικοινωνίας μεταξύ των επικοινωνούντων μερών του συστήματος. Τα λειτουργικά συστήματα επισκεπτών (guest operating systems) είναι συνδεδεμένα σε ένα διανομέα λογισμικού (software hub) τόσο για να επικοινωνούν μεταξύ τους όσο και για την επικοινωνία με τον διακομιστή. Όλοι οι πελάτες που είναι μέλη του ίδιου εικονικού δικτύου κάνουν χρήση της ίδιας εικονικής διεπαφής (virtual interface), εξυπηρετούνται από το ίδιο εικονικό μεταγωγέα (virtual switch) και η δικτυακή κυκλοφορία (network traffic) περνάει μέσα από την ίδια φυσική κάρτα δικτύου (physical network card).

Οι εικονικοί μεταγωγείς (virtual switches) κάνουν χρήση της λειτουργίας δρομολόγησης για να υλοποιήσουν την επικοινωνία μεταξύ των εικονικών μηχανών (virtual machines) με το μηχάνημα υποδοχής (host machine). Οπότε για την διεξαγωγή της επικοινωνίας απαιτείται μία εικονική διεπαφή (virtual interface), η Media Access Control (MAC) διεύθυνση που έχει εκχωρηθεί σε κάθε εικονική μηχανή (virtual machine) και η χρήση του πρωτοκόλλου Address Resolution Protocol (ARP) για την ανακατεύθυνση της κίνησης των εικονικών μηχανών (virtual machines) μέσω του δικτύου. Επιπλέον, διατηρούνται και πίνακες δρομολόγησης (routing tables) για την αποστολή μιας εντολής ARP σε κάθε εικονική μηχανή (virtual machine) κατά την διάρκεια του χρόνου εκκίνησης. Το πρωτόκολλο ARP είναι ευάλωτο σε ARP spoofing attack επειδή δεν απαιτεί απόδειξη της προέλευσης (proof-of origin) των συνομιλούντων μερών, ευπάθεια η οποία μπορεί να παραβιάσει την ασφάλεια του δικτύου επικοινωνίας και κατ΄ επέκταση την ασφάλεια του περιβάλλοντος εικονικοποίησης (virtualization) **[23]**.

3.10.2. Απειλές (Threats)

Η ARP spoofing attack είναι ένας τύπος παραβίασης σε δίκτυο υπολογιστών ο οποίος βασίζεται στο πρωτόκολλο ARP. Ο επιτιθέμενος μπορεί να αντιστοιχίσει οποιαδήποτε διεύθυνση MAC στην διεύθυνση IP του και να μεταδώσει λανθασμένα πακέτα ARP μπερδεύοντας τις εικονικές μηχανές (virtual machines) ώστε να στείλουν τα πλαίσια δεδομένων τους στην εικονική μηχανή (virtual machine) του επιτιθέμενου χωρίς να το αντιληφθούν. Άρα ο επιτιθέμενος έχει την δυνατότητα να χρησιμοποιήσει την επίθεση ARP spoofing attack έτσι ώστε να ανακατευθύνει όλη την κυκλοφορία της εικονικής μηχανής (virtual machine) «θύμα» στην δικιά του **[23]**. Επιπλέον, οι «παραδοσιακές» υπηρεσίας ασφαλείας δικτύων, όπως τα συστήματα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention Systems (IDPS)), δεν μπορούν να εντοπίσουν αν μία εικονική μηχανή (virtual machine) επιτίθεται σε κάποια άλλη μέσα στον ίδιο φυσικό διακομιστή, καθώς η κίνηση δεν περνάει μέσα από το φυσικό δίκτυο έτσι ώστε να μπορεί να αναλυθεί και να εντοπιστούν πιθανές επιθέσεις **[18]**.

Η απειλή που προκαλείται από την επίθεση ARP spoofing attack είναι ότι ο επιτιθέμενος έχει την δυνατότητα της κλοπής δεδομένων (data theft) αφού όλη η δικτυακή κίνηση της εικονικής μηχανής (virtual machine) «θύμα» περνάει από αυτόν. Επιπλέον, ο επιτιθέμενος μπορεί να προκαλέσει άρνηση υπηρεσίας (Denial of Service (DoS)) αφού έχει την δυνατότητα της μη δρομολόγησης και καταστροφής των πακέτων που φτάνουν σε αυτόν από την εικονική μηχανή (virtual machine) «θύμα» **[24]**.



Εικόνα 33 - ARP Spoofing Attack [75]

3.11. Έλλειψη Παρακολούθησης και Ελέγχου του Εσωτερικού Βασισμένου στο Λογισμικό Εικονικού Δικτύου

3.11.1. Ευπάθειες (Vulnerabilities)

Στα περιβάλλοντα εικονικοποίησης (virtualization) οι εικονικοί μεταγωγείς (virtual switches) δημιουργούνται για την υλοποίηση της επικοινωνίας των εικονικών μηχανών (virtual machines) μεταξύ τους. Εάν οι εικονικοί μεταγωγείς (virtual switches) δεν είναι ορθά παραμετροποιημένοι, «κακόβουλοι» χρήστες μπορούν να διεξάγουν επίθεση υποκλοπής της κίνησης του εικονικού δικτύου που περνάει μέσα από τον εικονικό μεταγωγέα (virtual switch) και κατευθύνεται προς τις υπόλοιπες εικονικές μηχανές (virtual machines) του δικτύου. Η επίθεση αυτή είναι γνωστή ως sniffing attack και προκαλείται από την ευπάθεια της έλλειψης παρακολούθησης και ελέγχου του εσωτερικού εικονικού δικτύου επικοινωνίας ενός συστήματος υπολογιστικού νέφους (cloud computing system) **[23]**. Επιπροσθέτως η κίνηση του δικτύου είναι πιθανών να μην είναι ορατή σε συστήματα προστασίας της ασφάλειας δικτύων, όπως τα συστήματα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention Systems (IDPS)), καθώς η κίνηση δεν περνάει μέσα

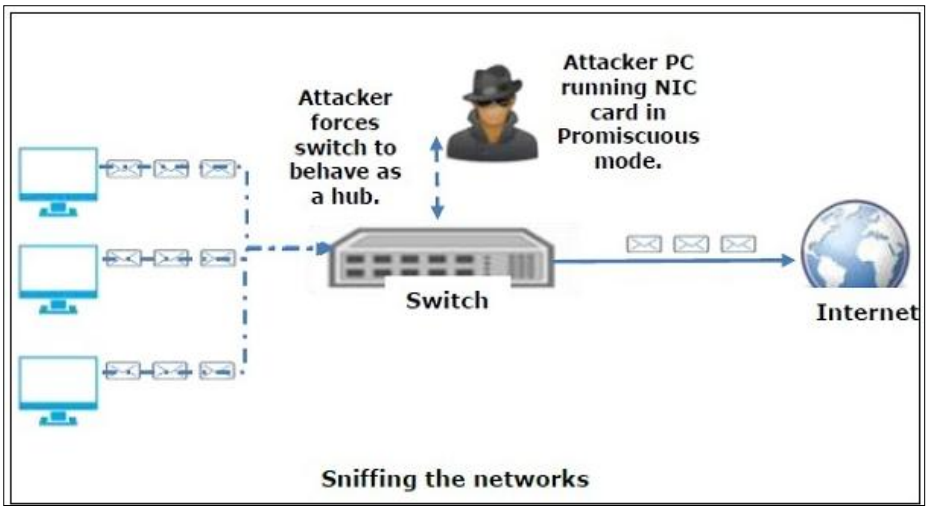
από το φυσικό δίκτυο έτσι ώστε να μπορεί να αναλυθεί και να εντοπιστούν πιθανές επιθέσεις.

Επομένως πιθανές αδυναμίες που μπορεί να οδηγήσουν στην ευπάθεια της έλλειψης παρακολούθησης και ελέγχου του εσωτερικού εικονικού δικτύου επικοινωνίας ενός συστήματος υπολογιστικού νέφους (cloud computing system) είναι:

- Έλλειψη παρακολούθησης του εικονικού δικτύου με πρακτικές που εφαρμόζονται στα φυσικά δίκτυα, όπως παραδείγματος χάριν λειτουργία συστήματος ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention Systems (IDPS)).
- Έλλειψη εφαρμογής συνεπής πολιτικής ασφαλείας στα φυσικά και στα εικονικά δίκτυα του συστήματος.
- Έλλειψη εφαρμογής συνολικής και ενιαίας παρακολούθησης των φυσικών και εικονικών δικτύων.
- Έλλειψη προσωπικού διαχείρισης και παραμετροποίησης των φυσικών και εικονικών δικτύων του συστήματος **[11]**.

3.11.2. Απειλές (Threats)

Σ’ ένα εικονικό δίκτυο μπορεί ο έλεγχος να γίνει μη διαχειρίσιμος αν η δικτυακή κίνηση δεν ανακατευθύνεται για παρακολούθηση και έλεγχο σε φυσικές ή εικονικές συσκευές με εγκατεστημένα δικτυακά εργαλεία ασφαλείας σχεδιασμένα γι᾽ αυτό τον σκοπό. Η απειλή, λοιπόν, που προκαλείται από μία επίθεση sniffing attack είναι ότι ο επιτιθέμενος παρακολουθώντας την δικτυακή κίνηση έχει την δυνατότητα της κλοπής δεδομένων (data theft), όπως κωδικούς πρόσβασης, κλειδιά κρυπτογράφησης κλπ., τα οποία μπορεί να χρησιμοποιήσει για «κακόβουλο» σκοπό και να θέση την ασφάλεια όλου του συστήματος σε κίνδυνο.



Εικόνα 34 - Sniffing Attack [76]

3.12. Μετανάστευση Εικονικών Μηχανών (Virtual Machines Migration)

3.12.1. Ευπάθειες (Vulnerabilities)

Σ' ένα περιβάλλον εικονικοποίησης (virtualization) που διαθέτει πολλαπλούς φυσικούς διακομιστές η μετακίνηση των εικονικών μηχανών (virtual machines) από τον έναν διακομιστή στον άλλον εξυπηρετεί ανάγκες εξισορρόπησης φορτίου (load balancing). Για παράδειγμα, εάν ένας διακομιστής έχει φτάσει στα όρια της εξάντλησης των πόρων του τότε μία ή περισσότερες εικονικές μηχανές (virtual machines) μπορούν να μετακινηθούν σε άλλο διακομιστή με λιγότερο φόρτο εργασίας. Με αυτό τον τρόπο βελτιώνεται η απόδοση και η διαθεσιμότητα των υπηρεσιών που προσφέρονται από τις εικονικές μηχανές (virtual machines) και παράλληλα γίνεται καλύτερη και ορθότερη κατανομή των πόρων **[12]**.

Οι εικονικές μηχανές (virtual machines) αποθηκεύονται σαν αρχεία κατά την διάρκεια της μετακίνησης τους από τον έναν διακομιστή στον άλλον και μπορούν να μεταφερθούν είτε μέσω δικτύου ή με την χρήση φυσικών

αποθηκευτικών μέσων. Αύτη η διαδικασία είναι γνωστή ως μετανάστευση εικονικών μηχανών (virtual machines migration) **[14]**.

Οι επιθέσεις κατά την διάρκεια της μετανάστευσης των εικονικών μηχανών (virtual machines migration) μπορούν να κατηγοριοποιηθούν σε τρία επίπεδα:

- Στο επίπεδο ελέγχου, επιθέσεις κατά του hypervisor που είναι υπεύθυνος για την επίβλεψη της διαδικασίας.
- Στο επίπεδο δεδομένων, ενεργητικές και παθητικές επιθέσεις στο κανάλι επικοινωνίας κατά την διάρκεια μεταφοράς των δεδομένων.
- Στο επίπεδο του migration module, τα κομμάτια του λογισμικού που χρησιμοποιούνται για να πραγματοποιηθεί η μετανάστευση των εικονικών μηχανών (virtual machines migration) ονομάζονται migration module και οι επιθέσεις έχουν σκοπό να μολύνουν αυτά τα τμήματα του λογισμικού **[14]**.

Οι επιθέσεις μπορούν να εκτοξευτούν με την αξιοποίηση των ακόλουθων ευπαθειών:

- Όταν η μετανάστευση της εικονικής μηχανής (virtual machine migration) γίνεται μέσω ενός ανασφαλή δικτύου.
- Όταν τα αρχεία της εικονική μηχανή (virtual machine) που μετακινείται είναι σε μορφή απλού κειμένου (clear text).
- Όταν η εικονική μηχανή (virtual machine) μεταφερθεί σε ένα μηχάνημα υποδοχής (host machine) το οποίο έχει παραβιάσει ο επιτιθέμενος.
- Όταν το περιεχόμενο της εικονικής μηχανής (virtual machine) που μετακινείται έχει μολυνθεί από επιβλαβή κώδικα **[25]**.

3.12.2. Απειλές (Threats)

Η μετανάστευση εικονικών μηχανών (virtual machines) χωρίς την τήρηση κανόνων ασφαλείας μπορεί να μετατραπεί σε μοναδικό σημείο αποτυχίας (single point of failure) για το σύστημα υπολογιστικού νέφους (cloud computing system) μέσα στο οποίο υλοποιείται.

Οι απειλές που μπορεί να προκληθούν σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) στο επίπεδο ελέγχου, έχοντας παραβιάσει ο επιτιθέμενος την ασφάλεια του hypervisor, είναι:

- Άρνησης υπηρεσίας (Denial of Service (DoS)) ενός άλλου «νόμιμου» hypervisor του συστήματος, μετακινώντας προς αυτόν μεγάλο αριθμό εικονικών μηχανών (virtual machines).
- Παραβίαση της ασφάλεια του hypervisor και των εικονικών μηχανών (virtual machine) του μηχανήματος υποδοχής (host machine), στο οποίο μεταναστεύει μία εικονική μηχανή (virtual machine), η οποία περιέχει «κακόβουλο» κώδικα.
- Ανακατεύθυνση των εικονικών μηχανών (virtual machine) που μετακινούνται στον υπολογιστή του επιτιθέμενου.
- Ψευδή διάθεση πόρων του μηχανήματος υποδοχής (host machine), του οποίου έχει θέσει σε κίνδυνο τον hypervisor, με σκοπό να επηρεάσει άλλα μηχανήματα υποδοχής του συστήματος να μεταναστεύσουν τις εικονικές μηχανές (virtual machines) τους προς αυτό για λόγους εξισορρόπησης φορτίου (load balancing).

Επιπλέον, οι απειλές που μπορούν να προκληθούν στο επίπεδο δεδομένων είναι απόρροια παθητικών και ενεργητικών επιθέσεων στο κανάλι επικοινωνίας κατά την διάρκεια της μεταφοράς των δεδομένων. Έτσι λοιπόν, οι απειλές από παθητικές και ενεργητικές επιθέσεις έχουν ως εξής:

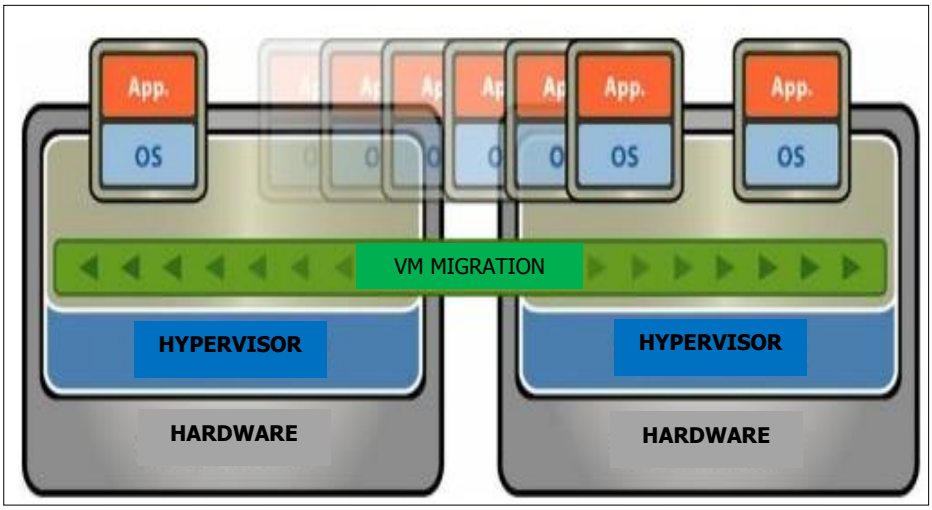
1. Απειλές από παθητικές επιθέσεις:
   - Διαρροή ευαίσθητων δεδομένων από την μνήμη της εικονικής μηχανής (virtual machine) που μετακινείται, όπως κλειδιά κρυπτογράφησης, κωδικοί πρόσβασης, δεδομένα εφαρμογών και άλλα.
   - Υποκλοπή (capturing) πακέτων αυθεντικοποίησης και επανυποβολή (replay) τους σε μεταγενέστερο χρόνο.
   - Εντοπισμός της εικονικής μηχανής (virtual machine) του επισκέπτη από την υποκλοπή δεδομένων μεγέθους και χαρακτηριστικών διάρκειας της μετανάστευσης.
   - Ο επιτιθέμενος είναι σε θέση να γνωρίζει την πηγή και τον προορισμό της διαδικασίας μετανάστευσης.

2. Απειλές από ενεργητικές επιθέσεις:

➢ Χειραγώγηση της μνήμης της εικονικής μηχανής (virtual machine) κατά την διάρκεια της μετανάστευσης.

➢ Χειραγώγηση των δεδομένων ειδικών εφαρμογών που αποθηκεύονται στην μνήμη της εικονικής μηχανής (virtual machine) κατά την διάρκεια της μετανάστευσης, όπως Secure Shell (SSH) και Pluggable Authentication Module (PAM).

Τέλος, η απειλή που μπορεί να προκληθεί σε ένα σύστημα λόγω παραβίασης του migration module είναι ότι ο επιτιθέμενος μπορεί να αποκτήσει τον πλήρη έλεγχο της διαδικασίας μετανάστευσης **[14]**.



Εικόνα 35 - Virtual Machines Migration [77]

3.13. Πολλαπλασιασμός Εικονικών Μηχανών (VM Sprawl)

3.13.1. Ευπάθειες (Vulnerabilities)

Η ευπάθεια του πολλαπλασιασμού εικονικών μηχανών (VM Sprawl) ορίζεται ως ένας μεγάλος αριθμός εικονικών μηχανών (virtual machines) μέσα σε ένα περιβάλλον υπολογιστικού νέφους (cloud computing) χωρίς την κατάλληλη διαχείριση. Ο πολλαπλασιασμός των εικονικών μηχανών (VM

Sprawl) είναι ένα από τα μεγαλύτερα προβλήματα που καλούνται να αντιμετωπίσουν πολλά κέντρα δεδομένων (data centers). Μια νέα εικονική μηχανή (virtual machine) μπορεί να δημιουργηθεί εύκολα και μέσα σε λίγα λεπτά με αποτέλεσμα η αύξηση των εικονικών μηχανών (VM Sprawl) να μην είναι απόλυτα προφανής, γεγονός που καταλήγει σε ένα περιβάλλον εικονικοποίησης (virtualization) με αρκετές δυσκολίες διαχείρισης λόγω του μεγάλου όγκου των εικονικών μηχανών (virtual machines) **[26]**.

Η ευπάθεια του VM Sprawl καταλήγει σε ανεξέλεγκτο πολλαπλασιασμό των εικονικών μηχανών (virtual machines) επειδή υπάρχει μεγάλη ευκολία τόσο στο να δημιουργηθεί μία νέα εικονική μηχανή (virtual machine) όσο και υπάρχουσες να κλωνοποιηθούν και να αντιγραφούν. Επιπροσθέτως, ο αριθμός των αδρανών εικονικών μηχανών (virtual machines) είναι πολύ πιθανόν να αυξηθεί και η μετακίνηση μίας εικονικής μηχανής (virtual machine) από το ένα μηχάνημα υποδοχής (host machine) στο άλλο πραγματοποιείται με μεγάλη ευκολία. Όλα αυτά έχουν σαν αποτέλεσμα την δημιουργία ενός περιβάλλοντος με μεγάλη πολυπλοκότητα ελέγχου και παρακολούθησης της ασφάλειας του. Απόρροια των ανωτέρω είναι μεγάλος όγκος εικονικών μηχανών να είναι μη ελέγξιμος (unmanaged), μη ενημερωμένος (unpatched) και μη ασφαλής (unsecured).

Αδυναμίες που μπορούν να οδηγήσουν στην ευπάθεια του ανεξέλεγκτου πολλαπλασιασμού των εικονικών μηχανών (VM Sprawl) είναι:

- Έλλειψη κατάλληλης πολιτικής και διαδικασιών ελέγχου με σκοπό την κατάλληλη διαχείριση του κύκλου ζωής των εικονικών μηχανών (virtual machines).
- Έλλειψη κατάλληλης πολιτικής διαχείρισης των αδρανών εικονικών μηχανών (virtual machines).
- Έλλειψη κατάλληλων εργαλείων για τον εντοπισμό μη εξουσιοδοτημένων εικονικών μηχανών (virtual machines) **[11]**.

3.13.2. Απειλές (Threats)

Η ευπάθεια του πολλαπλασιασμού των εικονικών μηχανών (VM Sprawl) προκαλείται από την ευκολία μιας εικονικής μηχανής (virtual machine) να δημιουργηθεί, να κλωνοποιηθεί, να αντιγραφεί και να μετακινηθεί. Οι απειλές που μπορεί να προκληθούν εξαιτίας του ανεξέλεγκτου πολλαπλασιασμού των εικονικών μηχανών (VM Sprawl) είναι ο ταχύτατος πολλαπλασιασμός εικονικών μηχανών (virtual machines) με άγνωστη παραμετροποίηση και ρυθμίσεις, η εξάντληση των πόρων του συστήματος που καταλήγει σε άρνηση υπηρεσίας (Denial of Service (DoS)), η υποβάθμιση (degrading) της συνολικής απόδοσης του συστήματος, η μη ύπαρξη αποτελεσματικού ελέγχου του συστήματος και η αύξηση της πιθανότητας εκθέσεως του συστήματος σε κίνδυνο.

Εικόνα 36 - Virtual Machines Sprawl [78]

4

Μέτρα Ασφαλείας

Μελετήσαμε στο Κεφάλαιο 3 τις ευπάθειες και τις απειλές των συστημάτων υπολογιστικού νέφους (cloud computing systems), τα οποία κάνουν χρήση της τεχνολογίας εικονικοποίησης (virtualization). Σε αυτό το Κεφάλαιο θα παρουσιάσουμε τα μέτρα ασφαλείας που πρέπει να υιοθετούνται από αυτά τα συστήματα με στόχο την αποφυγή και αν είναι δυνατόν την εξάλειψη των απειλών της εικονικοποίησης (virtualization).

Αρχικά στην ενότητα 4.1. θα παρουσιάσουμε τα γενικά μέτρα ασφαλείας που πρέπει να εφαρμόζονται σε κάθε σύστημα υπολογιστικού νέφους (cloud computing system) που κάνει χρήση των τεχνολογιών της εικονικοποίησης (virtualization) και στη συνέχεια στις ενότητες από 4.2. μέχρι 4.14. θα αναλύσουμε πιο συγκεκριμένα τα μέτρα ασφαλείας που πρέπει να εφαρμόζονται για κάθε μία ευπάθεια και αντίστοιχη απειλή που περιγράψαμε στο προηγούμενο Κεφάλαιο. Τέλος, στον **Πίνακας 2** θα παρουσιάσουμε μία αντιστοίχιση των ευπαθειών με τις απειλές που αυτές προκαλούν και τα αντίστοιχα μέτρα ασφαλείας που πρέπει να υιοθετούνται για την εξάλειψη των.

4.1. Γενικά Μέτρα Ασφαλείας για Περιορισμό των Κινδύνων σε Περιβάλλοντα Εικονικοποίησης (Virtualization)

Για να επιτευχθούν υψηλά επίπεδα ασφαλείας σ' ένα σύστημα υπολογιστικού νέφους (cloud computing system) που κάνει χρήση της τεχνολογίας εικονικοποίησης (virtualization) απαιτούνται:

1. Ύπαρξη πολιτικής ασφαλείας.
2. Θεσμοθέτηση κατάλληλων πρακτικών για την ενδυνάμωση και προστασία του υλικού (hardware), του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system), του hypervisor, της διεπαφής διαχείρισης (management interface) και των εικονικών μηχανών (virtual machines) από πιθανούς κινδύνους και απειλές.
3. Κατάλληλα μέτρα προστασίας για την ταχύτερη ανάκαμψη (recovery) και τη συνέχιση της λειτουργίας (continuity) του συστήματος από πιθανούς κινδύνους και καταστροφές.
4. Εφαρμογή κατάλληλων μηχανισμών ασφαλείας, όπως:

✓ Κρυπτογράφηση και διαχείριση κλειδιού (Encryption and Key Management (EKM)).

✓ Σύστημα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention System (IDPS)).

✓ Εικονικό Τείχος Προστασίας (Virtual Firewall (VF)).

✓ Trusted Virtual Domains (TVDs).

✓ Μηχανισμό ελέγχου πρόσβασης (Access Control Mechanisms (ACMs)).

✓ Virtual Trusted Platform Module (vTPM).

Ωστόσο, η ασφαλής ανάπτυξη ενός περιβάλλοντος εικονικοποίησης (virtualization) εκτός από την υλοποίηση μιας ασφαλούς και καλά σχεδιασμένης αρχιτεκτονικής και της ύπαρξης όλων των απαραίτητων λειτουργιών ασφαλείας απαιτεί τακτικούς ελέγχους ασφαλείας (regular

security audits) καθώς και δοκιμές διείσδυσης (penetration tests) για τον εντοπισμό άγνωστων ή νέου τύπου ευπαθειών και απειλών.

4.1.1. Πολιτική Ασφαλείας

Μια πολιτική ασφαλείας που ικανοποιεί τις ανάγκες του εκάστοτε περιβάλλοντος εικονικοποίησης (virtualization) πρέπει να εγκριθεί και να υιοθετηθεί. Η ανάπτυξη και θεσμοθέτηση της πολιτικής πρέπει να ακολουθήσει συγκεκριμένη μεθοδολογία αξιολογώντας τα επίπεδα εμπιστοσύνης μεταξύ των διαφόρων μερών του συστήματος, τις ζώνες ενεργείας των διαχειριστών καθώς και τα στοιχεία του υλικού και του λογισμικού. Αυτό απαιτεί:

- Καθορισμό των επιπέδων εμπιστοσύνης και διαχωρισμό των μηχανημάτων υποδοχής (host machines) αναλόγως του σκοπού για τον οποίο προορίζονται.
- Αξιολόγηση και διαχωρισμό των καθηκόντων των διαχειριστών με ταυτόχρονη δημιουργία διαφορετικών πολιτικών για διαχειριστές με διαφορετικές αρμοδιότητες, όπως παραδείγματος χάριν διαφορετικές πολιτικές για τους διαχειριστές των κέντρων δεδομένων (data center), τους διαχειριστές των εικονικών μηχανών (virtual machine) και τους διαχειριστές του hypervisor.
- Όπου οι απαιτήσεις ασφαλείας είναι διαφορετικές πρέπει να δημιουργήσουμε και ξεχωριστές ζώνες. Μόνο συστήματα με παρόμοιες απαιτήσεις ασφαλείας θα πρέπει να ομαδοποιούνται μέσα στο ίδιο μηχάνημα υποδοχής (host machine).

Μέσα σε αυτό το πλαίσιο απαιτείται επιπλέον να εξασφαλιστεί και η συνοχή της πολιτικής ασφαλείας καθώς θα πρέπει να τηρείται η ίδια πολιτική ανεξάρτητα παραδείγματος χάριν από το εάν μία εφαρμογή «τρέχει» μέσα σε λειτουργικό σύστημα εικονικής μηχανής (guest operating system) ή στο λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) **[2]**.

Εικόνα 37 - Πολιτική Ασφαλείας [79]

4.1.2. Μέτρα Ενδυνάμωσης και Προστασίας του Συστήματος

Τα μέτρα ενδυνάμωσης (hardening measures) είναι μέτρα βελτίωσης της ασφάλειας του εικονικού συστήματος με ταυτόχρονη μείωση της έκθεσης του σε ευπάθειες και απειλές. Σε γενικό πλαίσιο, ένα σύστημα μιας λειτουργίας είναι πιθανότατα πιο ασφαλές από ένα σύστημα πολλαπλών λειτουργιών. Έτσι λοιπόν όσο μεγαλύτερη είναι η επιφάνεια ευπάθειας τόσο μεγαλύτερη είναι και η έκθεση ενός εικονικού συστήματος σε απειλές.

Τα μέτρα ενδυνάμωσης (hardening measures), εντοπίζοντας τις ευπάθειες του συστήματος και προλαμβάνοντας τις απειλές, στοχεύουν στον εντοπισμό και προστασία όλων των δυνατών σημείων εισόδου (entry points) εκτόξευσης μιας επίθεσης (attack vectors). Διαδικασίες ενδυνάμωσης του εικονικού συστήματος, όπως η διαγραφή των ονομάτων χρηστών (usernames) και κωδικών πρόσβασης (passwords) καθώς και του λογισμικού που δεν χρησιμοποιούνται και η απενεργοποίηση των περιττών υπηρεσιών στοχεύουν να οδηγήσουν σε μία ισχυρή και με καλή διαχείριση πλατφόρμα, η οποία να παρέχει υπηρεσίες υψηλού επιπέδου στους χρήστες του εικονικού συστήματος. Ο **Πίνακας 1** παρουσιάζει μία σύνοψη των μέτρων

ενδυνάμωσης και προστασίας των συστημάτων υπολογιστικού νέφους (cloud computing systems) που βασίζονται στην εικονικοποίηση (virtualization) **[2]**.

Εικόνα 38 – Μέτρα Ενδυνάμωσης [80]

Πίνακας 1. Μέτρα Ενδυνάμωσης και Προστασίας του Συστήματος

ΚΑΤΗΓΟΡΙΕΣ	ΜΕΤΡΑ ΕΝΔΥΝΑΜΩΣΗΣ
Ασφάλεια Υλικού (Hardware)	• Χρήση διαδικασίας επικύρωσης (attestation) για επιβεβαίωση, όπου υποστηρίζεται. • Έλεγχος φυσικής πρόσβασης. • Χρήση κωδικού στο BIOS για αποτροπή επιθέσεων επανεκκίνησης. • Απομάκρυνση του υλικού που δεν χρησιμοποιείται.
Ασφάλεια Λειτουργικού Συστήματος Μηχανήματος Υποδοχής (Host Operating System)	• Χρήση διαδικασίας επικύρωσης (attestation) για επιβεβαίωση. • Εφαρμογή κοινά αποδεκτών (standard) διαδικασιών ενδυνάμωσης λειτουργικών συστημάτων: o Διαχείριση διορθώσεων (patches) και αλλαγών ελέγχου (control changes). o Πλήρης κρυπτογράφηση δίσκου, αν είναι δυνατό. o Απενεργοποίηση περιττών υπηρεσιών και διαγραφή λογισμικού που δεν χρησιμοποιείται. o Εγκατάσταση λογισμικού ανίχνευσης και αποτροπής εισβολών (Host IDPS) και λογισμικού ανίχνευσης ιών (Anti-Virus). o Εγκατάσταση βοηθητικού λογισμικού μόνο αν χρειάζεται. o Εφαρμογή διορθώσεων (patches) και ενημερώσεων (updates). • Εφαρμογή κοινά αποδεκτών (standard) μέτρων ασφάλειας δικτύων.
Ασφάλεια Hypervisor ή VMM	• Χρήση διαδικασίας επικύρωσης (attestation) και ελέγχων ακεραιότητας (integrity checks). • Εφαρμογή διορθώσεων, ενημερώσεων ασφαλείας και ενημερώσεων των καταχωρήσεων επικύρωσης (attestation records). • Έλεγχος και μεγάλη προσοχή στην κατανομή των πόρων στις εικονικές μηχανές (virtual machines). • Παρακολούθηση του hypervisor για πιθανές ενδείξεις που μπορούν να τον θέσουν σε κίνδυνο.
Ασφάλεια Διεπαφής Διαχείρισης (Management Interface)	• Μέτρα για την ελαχιστοποίηση της επιφάνειας επίθεσης είναι: o Απενεργοποίηση των διεπαφών, των δικτύων που δεν χρησιμοποιούνται και των τοπικών διαχειριστών. o Απαγόρευση πρόσβασης του τείχους προστασίας από μη αξιόπιστες περιοχές. o Διαχωρισμός του δικτύου διαχείρισης από τα άλλα προς χρήση δίκτυα, όπως το δίκτυο πυρήνα και το δίκτυο επισκεπτών. • Εφαρμογή ισχυρών έλεγχων αυθεντικοποίησης και εφαρμογή κρυπτογραφημένης επικοινωνίας. • Εφαρμογή περιορισμένων δικαιωμάτων πρόσβασης χρηστών. • Καταγραφή και έλεγχος συμβάντων. • Ασφάλεια των διεπαφών διαχείρισης του hypervisor τόσο τοπικά όσο και απομακρυσμένα. • Κρυπτογραφημένη επικοινωνία σε περίπτωση απομακρυσμένης διαχείρισης.

ΚΑΤΗΓΟΡΙΕΣ	ΜΕΤΡΑ ΕΝΔΥΝΑΜΩΣΗΣ
Ασφάλεια Εικονικών Μηχανών (Virtual Machines)	• Ενδυνάμωση των εικονικών μηχανών (virtual machines) με τις ίδιες πρακτικές που εφαρμόζονται και για τις φυσικές μηχανές: o Εφαρμογή διορθώσεων (patches) και ενημερώσεων ασφαλείας (updates). o Διαγραφή οδηγών (drivers) και λογισμικού που δεν χρησιμοποιείται. o Εγκατάσταση βοηθητικού λογισμικού μόνο αν χρειάζεται. o Απενεργοποίηση ή διαγραφή του εικονικού υλικού που δεν χρησιμοποιείται (K.M.E, RAM, οδηγοί πολυμέσων και άλλα). o Απαγόρευση εικονικών μηχανών (virtual machines) να κάνουν χρήση περισσότερων φυσικών πόρων από αυτούς που τους έχουν διατεθεί. o Εγκατάσταση λογισμικού ανίχνευσης ιών (Anti-Virus). • Ύπαρξη ελέγχου κατανομής των φυσικών πόρων. • Αποτροπή μη εξουσιοδοτημένης αντιγραφής με την χρήση μηχανισμών ασφαλείας επικύρωσης ταυτότητας (integrity validation), ελέγχου της υπογραφής (signature checking) και κρυπτογράφησης σε κάθε εικονική μηχανή (virtual machine). • Παρακολούθηση (monitor) των αλλαγών στις διαδικασίες διαχείρισης και παρακολούθηση (monitor) του ελέγχου εξ αποστάσεως. • Χρήση πρωτοκόλλου συγχρονισμού ασφαλούς χρόνου (secure time synchronization).

4.1.3. Μέτρα Προστασίας Ανάκαμψης (Recovery) και Συνέχισης (Continuity) της Λειτουργίας του Συστήματος

Σε ένα περιβάλλον εικονικοποίησης (virtualization) η ύπαρξη ενός σχεδίου ανάκαμψης (recovery) και συνέχισης (continuity) της λειτουργία του συστήματος είναι απαραίτητη. Επιπλέον, θα πρέπει να υπάρχουν σαφώς καθορισμένες διαδικασίες δημιουργίας αντιγράφων ασφαλείας (backup) και ανάκτησης του συστήματος, οι οποίες πρέπει να είναι στενά συνδεδεμένες με το επίπεδο κινδύνου που έχει ορίσει ο κάθε οργανισμό. Οι διαδικασίες ανάκτησης του συστήματος περιλαμβάνουν:

- Δημιουργία σε τακτικά χρονικά διαστήματα αντιγράφων ασφαλείας (backup).
- Ύπαρξη αυστηρών ελέγχων σε περιπτώσεις αλλαγών που σχετίζονται με τον τρόπο διαχείρισης του συστήματος.

- Ενοποίηση των ελέγχων ακεραιότητας (integrity) και επικύρωσης (attestation) **[2]**.

Εικόνα 39 - Αντίγραφα Ασφαλείας (Backups) [81]

4.1.4. Μηχανισμοί Ασφαλείας

Οι κυριότεροι μηχανισμοί ασφαλείας που πρέπει να εφαρμόζονται σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) που κάνει χρήση της τεχνολογίας εικονικοποίησης (virtualization) είναι οι παρακάτω:

- Κρυπτογράφηση και διαχείριση κλειδιού (Encryption and Key Management (EKM)).
- Σύστημα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention System (IDPS)).
- Εικονικό Τείχος Προστασίας (Virtual Firewall (VF)).
- Trusted Virtual Domains (TVDs).
- Μηχανισμό ελέγχου πρόσβασης (Access Control Mechanisms (ACMs)).
- Virtual Trusted Platform Module (vTPM).

Εικόνα 40 – Μηχανισμοί Ασφαλείας [82]

4.1.4.1. Κρυπτογράφηση και διαχείριση κλειδιού (Encryption and Key Management (EKM))

Η προστασία των δεδομένων από απώλεια ή κλοπή τους είναι κοινή ευθύνη τόσο του χρήστη όσο και του παρόχου σε συστήματα υπολογιστικού νέφους (cloud computing systems). Στις μέρες μας η κρυπτογράφηση είναι μία τεχνική που εφαρμόζεται σε όλες τις περιπτώσεις συμφωνητικών παροχής υπηρεσιών (service level agreement (SLA)) από παρόχους συστημάτων υπολογιστικού νέφους (cloud computing systems) **[4]**.

Τα ευαίσθητα δεδομένα των χρηστών πρέπει να κρυπτογραφούνται σε τρία διαφορετικά επίπεδα. Αρχικά, κατά την αποθήκευση, κρυπτογράφηση των δεδομένων κατά την αποθήκευση τους στον δίσκο σαν κρυπτογραφημένο κείμενο, το οποίο θα προστατεύσει τα δεδομένα τόσο από «κακόβουλους» χρήστες όσο και από παράνομη χρησιμοποίηση τους. Στην συνέχεια, κρυπτογράφηση τους κατά την μεταφορά τους, όπως κρυπτογράφηση παραδείγματος χάριν στοιχείων πιστωτικών καρτών ή άλλων ευαίσθητων δεδομένων κατά την μετάδοση τους μέσω του δικτύου. Τέλος, κρυπτογράφηση των δεδομένων των αντιγράφων ασφαλείας (backups), τα οποία αποθηκεύονται τόσο σε εξωτερικά όσο και σε εσωτερικά μέσα

αποθήκευσης, αυτό θα προστατεύσει τα δεδομένα των αντιγράφων ασφαλείας από κατάχρηση τόσο αν χαθούν όσο και αν κλαπούν.

Παρόλα αυτά η κρυπτογράφηση από μόνη της δεν μπορεί να εξασφαλίσει την ασφάλεια των δεδομένων, πρέπει παράλληλα με την κρυπτογράφηση να εφαρμόζονται και σωστές πρακτικές διαχείρισης κλειδιών για να εξασφαλίσουμε την ασφαλή και νόμιμη πρόσβαση στα κλειδιά κρυπτογράφησης. Έτσι λοιπόν, τα κλειδιά κρυπτογράφησης πρέπει να προστατεύονται με τον ίδιο τρόπο που προστατεύονται και τα ευαίσθητα δεδομένα και επιπλέον σε αυτά πρέπει να έχει πρόσβαση μόνο περιορισμένος αριθμός εξουσιοδοτημένων γι΄ αυτό τον σκοπό ατόμων και να ακολουθούνται κατάλληλες πρακτικές και διαδικασίες αν τα κλειδιά κρυπτογράφησης χαθούν ή κλαπούν.

Το είδος της τεχνικής κρυπτογράφησης που θα υλοποιηθεί σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) εξαρτάται από τις απαιτήσεις και τους στόχους του. Οι κοινές μέθοδοι κρυπτογράφησης που χρησιμοποιούνται σε μία εικονική υποδομή υπολογιστικού νέφους περιλαμβάνουν συμμετρική και ασύμμετρη κρυπτογράφηση. Αν οι πρακτικές κρυπτογράφησης δεδομένων ακολουθηθούν με ακρίβεια, αυτό θα συμβάλλει στην προστασία των δεδομένων από παράνομη πρόσβαση ή κλοπή από εσωτερικούς και εξωτερικούς «κακόβουλους» χρήστες **[20]**.

4.1.4.2. Σύστημα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention System (IDPS))

Ο μεγάλος αριθμός χρηστών (multi-tenant) και η κατανεμημένη φύση των συστημάτων υπολογιστικού νέφους (cloud computing systems) αποτελεί ελκυστικό στόχο «κακόβουλων» χρηστών. Επομένως, η εγκατάσταση συστημάτων ανίχνευσης και αποτροπής εισβολών (IDPS), κρίνεται αναγκαία, με στόχο τον εντοπισμό και τη παρεμπόδιση «κακόβουλων» ενεργειών. Τα σύστημα ανίχνευσης και αποτροπής εισβολών (IDPS) εντοπίζουν την εισβολή, την κατηγοριοποιούν και την ανατροφοδοτούν σε συσκευές ασφαλείας

προκειμένου να την αποτρέψουν, δημιουργώντας παράλληλα έναν κανόνα αντιμετώπισης της, αν αυτή εμφανιστεί ξανά. Επιπλέον, τα συστήματα ανίχνευσης και αποτροπής εισβολών (IDPS) μπορούν να χρησιμοποιηθούν και για άλλους σκοπούς όπως η τεκμηρίωση (documenting) υπαρχουσών απειλών, ο εντοπισμός προβλημάτων αναφορικά με την πολιτική ασφαλείας του συστήματος και η αποτροπή των χρηστών ηθελημένα ή μη να παραβιάσουν την πολιτική ασφαλείας **[2]**.

4.1.4.3. Εικονικό Τείχος Προστασίας (Virtual Firewall (VF))

Το εικονικό τείχος προστασίας (VF) πρόκειται για μια υπηρεσία που εκτελείται μέσα στο εικονικό περιβάλλον και η οποία λειτουργεί όπως ένα φυσικό τείχος προστασίας, φιλτράροντας τα πακέτα (packet filtering) και παρακολουθώντας τις υπηρεσίες (monitoring services). Το εικονικό τείχος προστασίας (VF) μπορεί να εκτελεστεί με διάφορους τρόπους λειτουργίας, όπως hypervisor-mode (hypervisor-based, hypervisor-resident) και bridge-mode. Για να προστατεύσει τον hypervisor και τις εικονικές μηχανές (virtual machines), το hypervisor-mode εικονικό τείχος προστασίας (VF) εγκαθίσταται στον hypervisor και είναι υπεύθυνο στο να συλλαμβάνει (capture) «κακόβουλες» ενέργειες κάνοντας χρήση όλων των γνωστών λειτουργιών του φυσικού τείχους προστασίας, όπως packet inspection, dropping και forwarding. Επιπλέον, το hypervisor-mode εικονικό τείχος προστασίας (VF) απαιτεί τροποποίηση στον πυρήνα (kernel) του hypervisor του μηχανήματος υποδοχής (host machine) για να μπορέσει να εγκαταστήσει άγκιστρα (hooks) και λειτουργίες (modules), τα οποία θα του επιτρέψουν να έχει πρόσβαση στις πληροφορίες των εικονικών μηχανών (virtual machines), στους εικονικούς μεταγωγείς δικτύου καθώς και σε όλες τις διεπαφές του εικονικού δικτύου για τον έλεγχο της μετακίνησης των πακέτων μεταξύ των εικονικών μηχανών (virtual machines) **[28]**.

4.1.4.4. Trusted Virtual Domains (TVDs)

Οι Trusted Virtual Domains (TVDs) είναι μία τεχνική ασφαλείας που εφαρμόζεται σε εικονικά συστήματα υπολογιστικού νέφους και η οποία ομαδοποιεί τις σχετικές εικονικές μηχανές (virtual machines), οι οποίες λειτουργούν σε ξεχωριστά φυσικά μηχανήματα, σε ένα ενιαίο τομέα δικτύου και κάτω από μία ενιαία πολιτική ασφαλείας. Οι εικονικές μηχανές (virtual machines) του ίδιου Trusted Virtual Domain (TVD) συνυπάρχουν σε μία ενιαία πλατφόρμα και κάτω από μία κοινή πολιτική πόρων και η ομαδοποίηση τους γίνεται με την επισήμανση τους με ένα μοναδικό αναγνωριστικό για κάθε εικονική μηχανή (virtual machine) του ίδιου Trusted Virtual Domain (TVD). Αυτή η τεχνική παρέχει ισχυρή απομόνωση μεταξύ των μη σχετικών εικονικών μηχανών (virtual machines) καθώς η επικοινωνία μεταξύ των Trusted Virtual Domains (TVDs) λαμβάνει χώρα βάση της πολιτικής ασφαλείας που έχει διαμορφωθεί από τον διαχειριστή του hypervisor του μηχανήματος υποδοχής (host machine). Με αυτό τον τρόπο μία «κακόβουλη» εικονική μηχανή (virtual machine) δεν μπορεί να εγγραφεί σε ένα Trusted Virtual Domain (TVD) γιατί θα πρέπει να πληροί τις απαιτήσεις της πολιτικής ασφαλείας **[20]**.

4.1.4.5. Μηχανισμός ελέγχου πρόσβασης (Access Control Mechanisms (ACMs))

Ο μηχανισμός ελέγχου πρόσβασης (ACM) προστατεύει ένα σύστημα καθώς περιορίζει ή απαγορεύει την πρόσβαση σε ένα σύστημα ή μία οντότητα σύμφωνα πάντα με την καθοριζόμενη πολιτική ασφαλείας. Οι πιο συχνά χρησιμοποιούμενοι μηχανισμοί ελέγχου πρόσβασης (ACMs) σε συστήματα υπολογιστικού νέφους (cloud computing systems) είναι οι Mandatory Access Control (Mac), Discretionary Access Control (DAC) και Role Based Access Control (RBAC) και είναι γνωστοί ως μηχανισμοί ελέγχου πρόσβασης (ACMs) βάση ταυτότητας δηλαδή βάση μοναδικού χαρακτηριστικού. Η αναγνώριση της ταυτότητας μπορεί να γίνει είτε απευθείας ή με την ανάθεση ρόλων και ο

μηχανισμός ουσιαστικά εγγυάται την ακεραιότητα και την εμπιστευτικότητα των πόρων. Επιπλέον, ο μηχανισμός ελέγχου πρόσβασης (ACM) πρέπει να υλοποιείται από μία έμπιστη οντότητα (trusted party), η οποία μπορεί να είναι είτε ο ίδιος ο πάροχος ή μία έμπιστη τρίτη οντότητα (trusted third party) **[20]**.

4.1.4.6. Virtual Trusted Platform Module (vTPM)

Ο μηχανισμός Virtual Trusted Platform Module (vTPM) βασίζεται σε μια αλυσίδα πιστοποιητικών, η οποία συνδέει τα vTPMs με το φυσικό TPM του μηχανήματος υποδοχής (host machine) προκειμένου να καταστεί διαθέσιμη η λειτουργία αυτού του μηχανισμού σε όλες τις εικονικές μηχανές (virtual machines) που λειτουργούν στο συγκεκριμένο μηχανήματος υποδοχής (host machine). Η λειτουργία αυτού του μηχανισμού βρίσκεται σε ένα συγκεκριμένο στρώμα πάνω από τον hypervisor και ο vTPM Manager δημιουργεί ένα vTPM για κάθε εικονική μηχανή (virtual machine). Ο vTPM Manager έχει εγκατασταθεί σε ένα συγκεκριμένο εικονικό μηχάνημα (virtual machine) με σκοπό να παρέχει vTPM στις εικονικές μηχανές και παίρνει το δικό του vTPM από τον hypervisor. Κάθε εικονική μηχανή (virtual machine) έχει το δικό της vTPM, το οποίο προσομοιώνει την λειτουργία του TPM του μηχανήματος υποδοχής (host machine). Για να επιτευχθεί, λοιπόν, αυτή η λειτουργία επεκτείνεται η αλυσίδα εμπιστοσύνης από το φυσικό TPM σε κάθε vTPM μέσω της προσεκτικής διαχείρισης των κλειδιών υπογραφής και των πιστοποιητικών και κάθε vTPM έχει το δικό του virtual Endorsement Key (EK) και virtual Storage Root Key (SRK). Σε ένα εικονικό περιβάλλον συστήματος υπολογιστικού νέφους μεγάλου αριθμού χρηστών (multi-tenant) ο μηχανισμός Virtual Trusted Platform Module (vTPM), λοιπόν, εικονοποιεί το φυσικό TPM του μηχανήματος υποδοχής (host machine) για να μπορεί να χρησιμοποιηθεί από έναν αριθμό εικονικών μηχανών (virtual machine) σε μία ενιαία πλατφόρμα υλικού **[20]**.

4.2. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Απομόνωσης Εικονικών Μηχανών (Isolation of Virtual Machines)

Για να αντιμετωπίσουμε τις ευπάθειες και τις απειλές, οι οποίες μπορούν να παραβιάσουν την απομόνωση των εικονικών μηχανών (virtual machines) με αποτέλεσμα να θέσουν σε κίνδυνο τη λειτουργία όλου του συστήματος απαιτούνται κατάλληλα μέτρα ασφαλείας. Έτσι λοιπόν, πρέπει να εφαρμόζονται όλα τα μέτρα ενδυνάμωσης που αναλύθηκαν στον **Πίνακας 1**. Επίσης, από τους μηχανισμούς ασφαλείας, οι οποίοι αναλύθηκαν στην ενότητα 4.1.4. αυτοί που συμβάλλουν καθοριστικά στην απομόνωση των εικονικών μηχανών (virtual machines) και πρέπει να εφαρμόζονται μέσα σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) είναι οι μηχανισμοί της κρυπτογράφησης και διαχείρισης κλειδιού (EKM) (ανατρέξτε στην ενότητα 4.1.4.1. για λεπτομέρειες), ο μηχανισμός Trusted Virtual Domains (TVDs) (ανατρέξτε στην ενότητα 4.1.4.4. για λεπτομέρειες), ο μηχανισμός ελέγχου πρόσβασης (ACM) (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες) και ο μηχανισμός Virtual Trusted Platform Module (vTPM) (ανατρέξτε στην ενότητα 4.1.4.6. για λεπτομέρειες).

4.3. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Διαφυγής Εικονικής Μηχανής (VM Escape) και Hyperjacking

Εάν ένας επιτιθέμενος κατορθώσει να διαφύγει από μία εικονική μηχανή (virtual machine) και αποκτήσει πρόσβαση στον hypervisor ή στο λειτουργικό σύστημα του μηχανήματος υποδοχής (host operating system) έχει την δυνατότητα να αποκτήσει πρόσβαση και στα λειτουργικά συστήματα όλων των εικονικών μηχανών (guests operating system). Επομένως, τα μέτρα

ασφαλείας που πρέπει να εφαρμοστούν για την αντιμετώπιση των απειλών VM escape και hyperjacking είναι:

- Επιλογή τύπου 1 hypervisor αντί για τύπου 2 (ανατρέξτε στην ενότητα 2.2.2. για λεπτομέρειες) καθώς έχει μικρότερο αποτύπωμα (footprint) με αποτέλεσμα την μείωση της επιφάνειας επίθεσης (attack surface) και κατ᾽ επέκταση την εμφάνιση λιγότερων ευπαθειών.
- Αποσύνδεση όλων των φυσικών συσκευών υλικού που δεν χρησιμοποιούνται καθώς και απενεργοποίηση του clipboard και της κοινής χρήσης αρχείων.
- Διενέργεια ελέγχου αυτό-ακεραιότητας (self-integrity checks) κατά την εκκίνηση (boot-up) για επιβεβαίωση αν ο hypervisor έχει παραβιαστεί ή όχι. Αυτό μπορεί να πραγματοποιηθεί με χρήση ανάλογης τεχνολογίας παρακολούθησης της ακεραιότητας του hypervisor, όπως παραδείγματος χάριν Trusted Platform Module/Trusted Execution Technology.
- Ανάλυση και έλεγχο των αρχείων καταγραφής (logs) του hypervisor για εντοπισμό πιθανών ενδείξεων που τον θέτουν σε κίνδυνο.
- Εγγραφή για λήψη όλων των ειδοποιήσεων και δελτίων ενημέρωσης ασφαλείας του παρόχου λογισμικού εικονικοποίησης (virtualization) και άμεση εφαρμογή όλων των ενημερώσεων (updates) και διορθώσεων (patches) ασφαλείας.
- Εφαρμογή αποτελεσματικού μηχανισμού ελέγχου πρόσβασης (ACM) σε όλα τα εργαλεία και εφαρμογές, τα οποία καλούν τον hypervisor μέσω διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces (APIs)).
- Εφαρμογή όλων των μέτρων ενδυνάμωσης ασφαλείας του hypervisor που αναφέρονται στον **Πίνακας 1 [11]**.

4.4. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της μη Εξουσιοδοτημένης Πρόσβασης στον Hypervisor ή VMM

Τα μέτρα ασφαλείας για να αποτρέψουμε την μη εξουσιοδοτημένη πρόσβαση στον hypervisor έχουν ως έξης:

- Εφαρμογή μηχανισμού ασφαλείας ελέγχου πρόσβασης βάση ρόλων (Role Based Access Control (RBAC)) για όλες τις δραστηριότητες διαχείρισης του hypervisor (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες). Επιπλέον, όλες οι δραστηριότητες διαχείρισης να ελέγχονται από περισσότερα του ενός ατόμων για μεγαλύτερο, ασφαλέστερο και αποτελεσματικότερο έλεγχο και εποπτεία.
- Αξιολόγηση και έλεγχο του εν λειτουργία μηχανισμού ασφαλείας ελέγχου πρόσβασης βάση ρόλων (Role Based Access Control (RBAC)) με την θεσμοθέτηση πολιτών ελέγχου πρόσβασης γι᾽ αυτόν τον σκοπό.
- Περιορισμό της πρόσβασης στο στρώμα εικονικοποίησης (virtualization) με την χρήση τείχους προστασίας (firewall), το οποίο να περιορίζει την πρόσβαση στην κονσόλα διαχείρισης του hypervisor. Το στρώμα εικονικοποίησης (virtualization) περιλαμβάνει τόσο το λογισμικό διαχείρισης του hypervisor όσο και τις διεπαφές προγραμματισμού εφαρμογών (Application Programming Interfaces (APIs)) και Command-Line Interfaces (CLIs).
- Περιορισμός στο ελάχιστο του αριθμού των λογαριασμών, οι οποίοι απαιτούν άμεση πρόσβαση στον hypervisor. Επιπλέον, λειτουργία ισχυρής διαχείρισης πιστοποιητικών και ελέγχων αυθεντικοποίησης για όλους τους λογαριασμούς χρηστών, τα οποία πρέπει να επιβάλλονται από την αντίστοιχη πολιτική ασφαλείας, όπως παραδείγματος χάριν πολιτικές κωδικού πρόσβασης και αυθεντικοποίηση με δυο διαφορετικούς τρόπους (2-factor authentication).
- Ύπαρξη κατάλληλης διαχείρισης και ελέγχου για κάθε αλλαγή που πραγματοποιείται σε κάθε στοιχείο του συστήματος προκειμένου να

αποφευχθεί η πιθανότητα η αλλαγή, κατά λάθος, να επιτρέψει μη εξουσιοδοτημένη πρόσβαση στον hypervisor.

- Απενεργοποίηση της απομακρυσμένη διαχείρισης του hypervisor, αν κάτι τέτοιο δεν είναι εφικτό θα πρέπει η πρόσβαση να γίνεται μέσω ασφαλούς σύνδεσης δικτύου και με χρήση αυθεντικοποίησης με δυο διαφορετικούς τρόπους (2-factor authentication). Επιπροσθέτως, θα πρέπει να οριστούν και πολιτικές διαχείρισης συνεδρίας (session), προκειμένου να τερματίζονται παραδείγματος χάριν αδρανείς ή ανενεργές συνδέσεις, για να αποτραπεί οποιαδήποτε ενδεχόμενο παραβίασης και να υπάρχουν κατάλληλοι μηχανισμοί ασφαλείας για κάθε τοπική και εξ αποστάσεως διεπαφή διαχείρισης, η οποία αποκτά πρόσβαση στον hypervisor.
- Ανάπτυξη ξεχωριστού δικτύου διαχείρισης (management LAN), το οποίο θα χρησιμοποιείται μόνο για την διαχείριση της πρόσβασης στον hypervisor.
- Εφαρμογή όλων των μέτρων ενδυνάμωσης ασφαλείας της διεπαφής διαχείρισης (Management Interface) που αναφέρονται στον **Πίνακας 1 [11]**.

4.5. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Εξάντλησης Πόρων (Resource Exhaustion)

Τα μέτρα ασφαλείας για την αντιμετώπιση των ευπαθειών και απειλών της εξάντλησης των φυσικών πόρων λόγω ταυτόχρονης χρήσης τους από πολλαπλές εικονικές μηχανές (virtual machines) έχουν ως έξης:

- Ύπαρξη κατάλληλων πολιτικών κατανομής και διατήρησης πόρων (resources), οι οποίες πρέπει να συμβαδίζουν με την κατηγοριοποίηση των εικονικών μηχανών (virtual machines) με βάση το επίπεδο ευαισθησίας ή κινδύνου τους.
- Εγκατάσταση λογισμικού ανίχνευσης ιών (Anti-Virus) τόσο εντός του περιβάλλοντος λειτουργίας των εικονικών μηχανών όσο και εκτός αυτού.

- Εγκατάσταση μηχανισμών για την ελαχιστοποίηση της εξάντλησης πόρων (resource contention).
- Καθορισμό και εφαρμογή τυποποιημένης διαδικασίας για τον εντοπισμό εικονικών μηχανών (virtual machines), οι οποίες είναι σε αναμονή λειτουργίας λόγω της εξάντλησης των πόρων τους και εφαρμογή άμεσης λύσης αποκατάστασης της λειτουργίας τους **[11]**.

4.6. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών των Αδρανών (Dormant) ή Εκτός Λειτουργίας (Offline) Εικονικών Μηχανών (Virtual Machines)

Οι αδρανείς (dormant - suspended), εκτός λειτουργίας (offline - shut down) και οι εικονικές μηχανές (virtual machines) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας μπορεί να απέχουν πάρα πολύ από την τρέχουσα κατάσταση ασφαλείας με αποτέλεσμα να είναι ευάλωτες σε μεγάλο αριθμό ευπαθειών παραβίασης της ασφάλειας τους. Τα μέτρα ασφαλείας για την αντιμετώπιση της μη έγκαιρης ενημέρωση του λογισμικού αυτών των εικονικών μηχανών είναι:

- Δημιουργία ελεγχόμενου περιβάλλοντος εφαρμογής των διορθώσεων (patches) και ενημερώσεων (updates) ασφαλείας με ταυτόχρονο καθορισμό πολιτικών ελέγχου στις αδρανείς, εκτός λειτουργίας και στις εικονικές μηχανές (virtual machines) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας.
- Ενημέρωση με τις τελευταίες διορθώσεις (patches) και ενημερώσεις (updates) ασφαλείας όλων των εικονικών μηχανών (virtual machines) ενεργών, αδρανών, εκτός λειτουργίας και αυτών που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας κάνοντας χρήση κατάλληλου open source ή commercial λογισμικού, το οποίο προσφέρει λύσεις διαχείρισης.

- Κατάλληλη αρχιτεκτονική, σχεδιασμό και ταυτόχρονα συνεχείς ελέγχους των εικονικών συσκευών, οι οποίες παρέχουν κρίσιμες υπηρεσίες υποδομών, διαχείρισης και ασφαλείας για την αποφυγή προβλημάτων με αδρανής και εκτός λειτουργίας εικονικές μηχανές (virtual machines) **[11]**.

4.7. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών των Προ-Ρυθμισμένων (Pre-Configured) Εικονικών Μηχανών (Virtual Machines)

Η έλλειψη διασφάλισης της ακεραιότητας των προ-ρυθμισμένων (pre-configured) εικονικών μηχανών (virtual machines) είναι μία σοβαρή ευπάθεια και τα μέτρα ασφαλείας για την αντιμετώπιση της είναι:

- Εφαρμογή μηχανισμού ελέγχου ακεραιότητας (integrity checksum mechanism) των προ-ρυθμισμένων εικονικών μηχανών (virtual machines).
- Κρυπτογράφηση των εικόνων (images) των προ-ρυθμισμένων εικονικών μηχανών (virtual machines) για την αποτροπή μη εξουσιοδοτημένης τροποποίησης τους (ανατρέξτε στην ενότητα 4.1.4.1. για λεπτομέρειες).
- Εφαρμογή αυστηρών ελέγχων και διαδικασιών αναφορικά με την πρόσβαση (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες), την δημιουργία και την ανάπτυξη τόσο στις εικόνες (images) των προ-ρυθμισμένων εικονικών μηχανών (virtual machines) όσο και στις ίδιες τις εικονικές μηχανές (virtual machines). Πριν την δημιουργία μιας νέας εικόνας (image) να γίνεται έλεγχος αυτής με σάρωση και φιλτράρισμα για ύπαρξη «κακόβουλου» κώδικα και ταυτόχρονα καταγραφή όλων των ενεργειών.
- Εγκατάσταση και χρήση διαφόρων εμπορικών εργαλείων παρακολούθησης και ελέγχων καθώς και εκμετάλλευση των ήδη υπαρχόντων προ-εγκατεστημένων εργαλείων των λειτουργικών συστημάτων με σκοπό την ταυτόχρονη λειτουργία πολυεπίπεδων ελέγχων ασφαλείας.
- Εφαρμογή όλων των μέτρων ενδυνάμωσης ασφαλείας των εικονικών μηχανών (virtual machines) που αναφέρονται στον **Πίνακας 1 [11]**.

4.8. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών των Ευαίσθητων Δεδομένων Μέσα στις Εικονικές Μηχανές (Virtual Machines)

Τα ευαίσθητα δεδομένα που είναι αποθηκευμένα μέσα στις εικονικές μηχανές (virtual machines) αποθηκεύονται και μέσα στις αντίστοιχες από αυτές εικόνες (images) και στιγμιότυπα (snapshots). Τα μέτρα ασφαλείας που πρέπει να παρθούν για να εξαλείψουμε τον κίνδυνο ευαίσθητα δεδομένα να περάσουν στα χέρια «κακόβουλων» χρηστών είναι:

- Κρυπτογράφηση όλων των δεδομένων των εικονικών μηχανών (virtual machines) και του μηχανήματος υποδοχής (host machine) ώστε να μην μπορούν να αναγνωστούν (ανατρέξτε στην ενότητα 4.1.4.1. για λεπτομέρειες). Επιπλέον, εφαρμογή ισχυρών ελέγχων ακεραιότητας και ταυτότητας όταν μία εικονική μηχανή (virtual machine) αιτείται πρόσβαση σε ασφαλής περιοχές αποθήκευσης (secure storage volumes). Θα πρέπει επίσης οι τόμοι εκκίνησης και δεδομένων (boot and data volume) να είναι κρυπτογραφημένοι.
- Ύπαρξη πολιτικής, η οποία να περιορίζει την αποθήκευση εικόνων (images) και στιγμιότυπων (snapshots). Στην περίπτωση όμως που μία εικόνα (image) ή ένα στιγμιότυπο (snapshots) αποθηκεύεται θα πρέπει να υπάρχουν κατάλληλες διαδικασίες παρακολούθησης και ελέγχου και κατάλληλη εξουσιοδότηση. Επιπλέον, ύπαρξη κατάλληλων πολιτικών και διαδικασιών διαχείρισης των εικόνων (images) αναφορικά με τον τρόπο δημιουργίας, ασφαλείας, διανομής, αποθήκευσης, χρήσης, θέσεως τους εκτός ενεργείας και καταστροφής τους.
- Ύπαρξη πολιτικής διαγραφής των δεδομένων και των εικόνων (images) που παραμένουν στην προηγούμενη τους θέση όταν μία εικονική μηχανή (virtual machine) μεταναστεύσει (migrate) από το ένα φυσικό μηχάνημα στο άλλο.
- Εφαρμογή προστασίας με την ύπαρξη ελέγχου επιβεβαίωσης του αθροίσματος έλεγχου κρυπτογράφησης (cryptographic checksum) για τον

εντοπισμό αλλαγών σε εικόνες (images) και στιγμιότυπα (snapshots) εικονικών μηχανών (virtual machines).

- Ύπαρξη μηχανισμού για τον έλεγχο της πρόσβασης σε κάθε εικόνα (image) και εικονική μηχανή (virtual machine) (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες) προκειμένου να αποτραπεί από έναν επιτιθέμενο η δυνατότητα δημιουργίας ή παραγωγής «μολυσμένης» εικόνας (image). Επιπλέον πριν την δημιουργία μιας νέας εικόνας (image) ή χρήση μιας ήδη υπάρχουσας να γίνεται έλεγχος αυτής με σάρωση και φιλτράρισμα για ύπαρξη «κακόβουλου» κώδικα και ταυτόχρονα καταγραφή όλων των ενεργειών.
- Ύπαρξη ελέγχων για εντοπισμό κρίσιμων δεδομένων μέσα σε εικονικές μηχανές (virtual machines), τα οποία μπορεί να χρήζουν μεγαλύτερο βαθμό παρακολούθησης και ελέγχου **[11]**.

4.9. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών του Μικτού Επιπέδου Εμπιστοσύνης Εικονικών Μηχανών (Virtual Machines)

Εικονικές μηχανές (virtual machines) στις οποίες είναι αποθηκευμένα ευαίσθητα δεδομένα μπορεί να βρίσκονται μέσα στο ίδιο μηχάνημα υποδοχής (host machine) μαζί με άλλες στις οποίες είναι αποθηκευμένα λιγότερο κρίσιμα δεδομένα. Αυτό έχει σαν αποτέλεσμα την δημιουργία ενός μικτού επιπέδου εμπιστοσύνης εικονικών μηχανών (virtual machines). Τα μέτρα ασφαλείας για την αντιμετώπιση των ευπαθειών και απειλών της δημιουργίας μικτών επιπέδων εμπιστοσύνης εικονικών μηχανών (virtual machines) είναι:

- Εφαρμογή διαδικασιών για την ταξινόμηση των συστημάτων και δεδομένων με βάση την ταξινόμηση που έχει οριστεί από την πολιτική ασφαλείας.
- Διαχωρισμό των χρηστών, με βάση τον φόρτο εργασίας τους, σε διαφορετικά επίπεδα εμπιστοσύνης και σε διαφορετικά εικονικά δίκτυα (VLANs) και αν είναι εφικτό σε διαφορετικούς φυσικούς και λογικούς

διακομιστές, στους οποίους θα εφαρμόζονται και διαφορετικές πολιτικές ασφαλείας.

- Δημιουργία διαφορετικών επιπέδων εμπιστοσύνης για τα διαφορετικά φυσικά και λογικά δίκτυα. Επιπλέον, εξέταση της δυνατότητας διαχωρισμού των εικονικών μηχανών (virtual machines) με την δημιουργία ζωνών ασφαλείας ανάλογα με τον σκοπό που χρησιμοποιούνται και την ευαισθησία των δεδομένων που περιέχουν.
- Ανάπτυξη φυσικών και εικονικών τείχων προστασίας (firewalls) για απομόνωση ομάδων εικονικών μηχανών (virtual machines) ανάλογα με την ομάδα εργασίας που ανήκουν μέσα στο μηχάνημα υποδοχής (host machine). Παραδείγματος χάριν διαχωρισμός των εικονικών μηχανών (virtual machines) που ανήκουν στην ομάδα παραγωγής από αυτές της ομάδας ανάπτυξης.
- Προσεκτικός σχεδιασμός και υλοποίηση της πρόσβασης σε φυσικά και εικονικά συστήματα διαχείρισης και ασφαλείας από κάθε επίπεδο εμπιστοσύνης **[11]**.

4.10. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών του Περάσματος από την μία Εικονική Μηχανή στην Άλλη (VM Hopping)

Τα μέτρα ασφαλείας για την απαγόρευση μιας εικονικής μηχανής (virtual machine) να πάρει τον έλεγχο μιας άλλης εικονικής μηχανής (virtual machine) εκμεταλλευόμενη αδυναμίες του επιπέδου εμπιστοσύνης μεταξύ των εικονικών μηχανών (virtual machines) είναι τα μέτρα ενδυνάμωσης ασφαλείας των εικονικών μηχανών (virtual machines) που αναφέρονται στον **Πίνακας 1 [2]**.

4.11. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Address Resolution Protocol (ARP) Spoofing Attack

Τα μέτρα ασφαλείας που πρέπει να ληφθούν για την αντιμετώπιση της επίθεσης ARP spoofing είναι:

- Λειτουργία εικονικού τείχους προστασίας (VF) (ανατρέξτε στην ενότητα 4.1.4.3. για λεπτομέρειες), το οποίο φιλτράρει και επιθεωρεί τα πακέτα που μεταδίδονται σε ένα δίκτυο. Η λειτουργία του φιλτραρίσματος των πακέτων (packet filtering) είναι σημαντική στην αντιμετώπιση της επίθεσης IP address spoofing επειδή έχει την δυνατότητα να φιλτράρει και να μπλοκάρει πακέτα με αντικρουόμενες πληροφορίες για την διεύθυνση πηγής, όπως παραδείγματος χάριν πακέτα που προέρχονται από το εξωτερικό δίκτυο και δείχνουν διευθύνσεις πηγής του εσωτερικού δικτύου και αντίστροφα.
- Αποφυγή όσο είναι δυνατόν σχέσεων εμπιστοσύνης με την ανάπτυξη αντίστοιχων πρωτοκόλλων. Οι σχέσεις εμπιστοσύνης χρησιμοποιούν για τον έλεγχο ταυτότητας μόνο τις διευθύνσεις IP και άρα είναι πιο εύκολο για έναν επιτιθέμενο να διεξάγει μία επίθεση ARP spoofing.
- Εγκατάσταση open source ή commercial λογισμικού για εντοπισμό επιθέσεων spoofing.
- Χρήση πρωτοκόλλων κρυπτογράφησης δικτύου, όπως Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS), IPsec και άλλα πρωτόκολλα ασφαλούς επικοινωνίας, τα οποία ενισχύουν την ασφάλεια κατά των επιθέσεων ARP spoofing αφού κρυπτογραφούν τα δεδομένα πριν την αποστολή τους και εφαρμόζουν μεθόδους αυθεντικοποίησης μόλις αυτά φτάσουν στον προορισμό τους **[29]**.

4.12. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Έλλειψη Παρακολούθησης και Ελέγχου του Εσωτερικού Βασισμένου στο Λογισμικό Εικονικού Δικτύου

Για την αντιμετώπιση των ευπαθειών και απειλών της έλλειψη παρακολούθησης και ελέγχου του εσωτερικού βασισμένου στο λογισμικό εικονικού δικτύου απαιτούνται κατάλληλα μέτρα ασφαλείας, τα οποία είναι:

- Ύπαρξη συνεπής πολιτικής ασφαλείας και παραμετροποιήσεων και για τα εικονικά και για τα φυσικά δίκτυα.
- Παρακολούθηση των εικονικών δικτύων και της διαβίβασης δεδομένων τους με πρακτικές που εφαρμόζονται στα φυσικά δίκτυα, όπως το εικονικό τείχος προστασίας (VF) (ανατρέξτε στην ενότητα 4.1.4.3. για λεπτομέρειες) και τα συστήματα ανίχνευσης και αποτροπής εισβολών (IDPS) (ανατρέξτε στην ενότητα 4.1.4.2. για λεπτομέρειες).
- Χρήση τεχνολογιών ασφαλείας που να λειτουργούν με τον ίδιο τρόπο τόσο στα φυσικά όσο και στα εικονικά περιβάλλοντα κάτω από το ίδιο πλαίσιο εφαρμογής και ακλουθώντας την ίδια πολιτική για την διαχείρισης τους.
- Ενσωμάτωση στις διεπαφές προγραμματισμού εφαρμογών (APIs) του hypervisor εξειδικευμένων μηχανισμών ασφαλείας για την παροχή παρακολούθησης και ελέγχου της κυκλοφορίας των δεδομένων των εικονικών μηχανών (virtual machines). Τέτοιου είδους μηχανισμοί ασφαλείας είναι οι τεχνολογίες Software-Defined Network (SDN) και OpenFlow **[11]**.

4.13. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών της Μετανάστευσης Εικονικών Μηχανών (Virtual Machines Migration)

Η μετανάστευση εικονικών μηχανών (virtual machines) χωρίς την τήρηση κανόνων ασφαλείας μπορεί να μετατραπεί σε μοναδικό σημείο αποτυχίας (single point of failure) για το σύστημα υπολογιστικού νέφους (cloud computing system). Επομένως τα μέτρα ασφαλείας για την ασφαλή διαδικασία μετανάστευση των εικονικών μηχανών (virtual machines) από το ένα μηχάνημα υποδοχής (host machine) στο άλλο είναι:

- Υλοποίηση ελέγχου ακεραιότητας του μηχανήματος υποδοχής (host machine) προορισμού, δηλαδή το μηχάνημα υποδοχής (host machine) προορισμού ταυτοποιεί με κρυπτογραφική διαδικασία τον εαυτό του στο μηχάνημα υποδοχής (host machine) πηγής για την εγκαθίδρυση της μεταξύ τους σχέσεως εμπιστοσύνης.
- Ύπαρξη έλεγχου αυθεντικοποίησης έτσι ώστε να αποτρέψει σε έναν επιτιθέμενο να διενεργήσει μία επίθεση Man in the Middle (MITM), όπως παραδείγματος χάριν route hijacking ή ARP poisoning κατά την διαδικασία της μετανάστευσης. Προκειμένου να επιτευχθεί αυτό πρέπει τα μηχανήματα υποδοχής (host machines) πηγής και προορισμού να διενεργήσουν αμοιβαία αυθεντικοποίηση (mutually authenticate).
- Ύπαρξη κατάλληλης πολιτικής ελέγχου πρόσβασης (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες) για την διασφάλιση της διαδικασίας μετανάστευσης και την επίτευξη της εξουσιοδότησης, δηλαδή ποιος μπορεί να κάνει κάτι και τι είναι αυτό, ώστε ένας μη εξουσιοδοτημένος χρήστης να μην μπορεί να επέμβει στην διαδικασία μετανάστευσης.
- Ύπαρξη εμπιστευτικότητας και ακεραιότητας κατά την διάρκεια της μετανάστευσης των εικονικών μηχανών (virtual machines) με την εγκαθίδρυση ενός κρυπτογραφημένου καναλιού επικοινωνίας. Με αυτό τον τρόπο ένας επιτιθέμενος δεν μπορεί να υποκλέψει οποιαδήποτε πληροφορία για τα περιεχόμενα των εικονικών μηχανών (virtual machines) ούτε να

τροποποιήσει το περιεχόμενο τους. Έτσι μπορούμε να αποτρέψουμε και τις παθητικές και τις ενεργητικές επιθέσεις.

- Η διαδικασία μετανάστευσης πρέπει να είναι ανθεκτική σε επαναλήψεις (replay resistance) έτσι ώστε ένας επιτιθέμενος να μην μπορεί να αντιγράψει την κίνηση του δικτύου με σκοπό σε μεταγενέστερο χρόνο να την επαναλάβει (replay) για να αποκτήσει πρόσβαση στην διαδικασία μετανάστευσης.
- Χρήση πιστοποιητικών δημόσιου κλειδιού έτσι ώστε η πηγή να μην μπορεί να αρνηθεί (non-repudiation) την μετανάστευση της εικονικής μηχανής (virtual machine) **[14]**.

4.14. Μέτρα ασφαλείας για την Αντιμετώπιση των Ευπαθειών και Απειλών του Πολλαπλασιασμού Εικονικών Μηχανών (VM Sprawl)

Η ύπαρξη μεγάλου αριθμού εικονικών μηχανών (virtual machines) καταλήγει σε ανεξέλεγκτο πολλαπλασιασμό τους με αποτέλεσμα την δημιουργία ενός περιβάλλοντος με μεγάλη πολυπλοκότητα στον έλεγχο και στην παρακολούθηση της ασφάλειας που οδηγεί σε απώλεια ελέγχου. Τα μέτρα ασφαλείας για την αντιμετώπιση αυτής της κατάστασης είναι:

- Ύπαρξη κατάλληλων πολιτικών, κατευθυντήριων γραμμών και διαδικασιών με σκοπό την κατάλληλη διαχείριση και έλεγχο του κύκλου ζωής των εικονικών μηχανών (virtual machines).
- Έλεγχος της δημιουργίας, αποθήκευσης και χρήσης των εικόνων (images) των εικονικών μηχανών (virtual machines) με κατάλληλα εργαλεία και ταυτόχρονη ύπαρξη διαδικασιών διαχείρισης αλλαγών. Νέες προσθήκες θα πρέπει να γίνονται μόνο όταν είναι απαραίτητο.
- Διατήρηση ξεχωριστά ενός μικρού σε αριθμό, ενημερωμένων και ορθά ρυθμισμένων εικόνων (images) των λειτουργικών συστημάτων των

επισκεπτών (guest operating systems), οι οποίες θα χρησιμοποιηθούν για την γρήγορη ανάκαμψη και συνέχιση της λειτουργίας του συστήματος.

- Ύπαρξη πολιτικής διαχείρισης και εντοπισμού των αδρανών εικονικών μηχανών (virtual machines) με την ύπαρξη κατάλληλων ελέγχων ασφαλείας σε κάθε εικονική μηχανή (virtual machine) και των αντιστοιχών συνδέσεων δικτύου της.
- Χρήση προϊόντων εικονικοποίησης (virtualization) που προσφέρουν λύσεις διαχείρισης, έτσι ώστε να εξετάζουν, διορθώνουν (patch) και να εφαρμόζουν τις αλλαγές διαμόρφωσης ασφαλείας σε όλες τις εικονικές μηχανές (virtual machines) **[11]**.

Πίνακας 2. Συγκεντρωτικός Πίνακας Ευπαθειών – Απειλών και Μέτρων Ασφαλείας

ΚΑΤΗΓΟΡΙΕΣ	ΕΥΠΑΘΕΙΕΣ	ΑΠΕΙΛΕΣ	ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ
Hypervisor ή VMM	Απομόνωση εικονικών μηχανών: 1. Πρόσβαση όλων των εικονικών μηχανών στους ίδιου φυσικούς πόρους. 2. Δέσμευση περισσότερων πόρων από αυτούς που έχουν διατεθεί (VM poaching attack).	1. Διαρροή δεδομένων (data leakage). 2. α. Άρνηση υπηρεσίας (DoS). β. Διακοπή του Συστήματος.	Όπως περιγράφονται στην παράγραφο 4.2..
	Διαφυγή εικονικής μηχανής (VM Escape) και Hyperjacking.	α. Έλεγχος όλων των εικονικών μηχανών που «τρέχουν» στο συγκεκριμένο hypervisor ή στο συγκεκριμένο μηχάνημα υποδοχής. β. Παραβίαση της ασφάλεια των hypervisors με τους οποίους αλληλεπιδρά ο συγκεκριμένος hypervisor.	Όπως περιγράφονται στην παράγραφο 4.3..
	Όπως περιγράφονται στην παράγραφο 3.3.1..	Μη Εξουσιοδοτημένη Πρόσβαση στον Hypervisor.	Όπως περιγράφονται στην παράγραφο 4.4..
	Εξάντληση των φυσικών πόρων λόγω ταυτόχρονης χρήσης τους από πολλαπλές εικονικές μηχανές.	Άρνηση υπηρεσίας (DoS).	Όπως περιγράφονται στην παράγραφο 4.5..

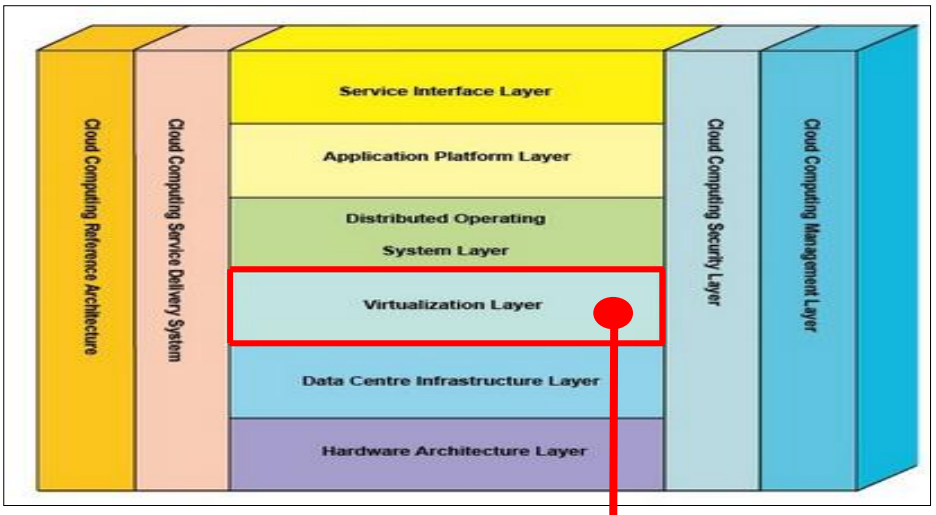
ΚΑΤΗΓΟΡΙΕΣ	ΕΥΠΑΘΕΙΕΣ	ΑΠΕΙΛΕΣ	ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ
Εικονικές Μηχανές (Virtual Machines)	Μη έγκαιρη ενημέρωση του λογισμικού των αδρανών, εκτός λειτουργίας εικονικών μηχανών και αυτών που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας με τις πιο πρόσφατές ενημερώσεις (updates) και διορθώσεις (patches).	Κλοπή δεδομένων (data theft).	Όπως περιγράφονται στην παράγραφο 4.6..
	Έλλειψη διασφάλισης της ακεραιότητας των προ-ρυθμισμένων εικονικών μηχανών.	Απώλειας ακεραιότητας (loss of integrity).	Όπως περιγράφονται στην παράγραφο 4.7..
	Ευαίσθητα Δεδομένα Μέσα στις Εικονικές Μηχανές (Όπως περιγράφονται στην παράγραφο 3.7.1.).	Απώλεια ευαίσθητων δεδομένων (sensitive data theft).	Όπως περιγράφονται στην παράγραφο 4.8..
	Μικτό επίπεδο εμπιστοσύνης εικονικών Μηχανών (Όπως περιγράφονται στην παράγραφο 3.8.1.).	Μείωση της συνολικής ασφάλειας του συστήματος σε εκείνη που ισχύει για τα λιγότερο προστατευμένα στοιχεία του.	Όπως περιγράφονται στην παράγραφο 4.9..
	Πέρασμα από την μία εικονική μηχανή στην άλλη (VM Hopping).	α. Έλεγχο του λειτουργικού συστήματος της εικονικής μηχανής που έχει θέσει υπό τον έλεγχο του. β. Άρνηση υπηρεσίας (DoS).	Όπως περιγράφονται στην παράγραφο 4.10..

ΚΑΤΗΓΟΡΙΕΣ	ΕΥΠΑΘΕΙΕΣ	ΑΠΕΙΛΕΣ	ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ
Δίκτυο Επικοινωνίας (Network Communication)	Επίθεση Address Resolution Protocol (ARP) Spoofing.	α. Κλοπή δεδομένων (data theft). β. Άρνηση υπηρεσίας (DoS).	Όπως περιγράφονται στην παράγραφο 4.11..
	Έλλειψη παρακολούθησης και ελέγχου του εσωτερικού εικονικού δικτύου επικοινωνίας (Όπως περιγράφονται στην παράγραφο 3.11.1.).	Κλοπή δεδομένων (data theft).	Όπως περιγράφονται στην παράγραφο 4.12..
Ρυθμίσεις (Configuration)	Μετανάστευση εικονικών μηχανών (Όπως περιγράφονται στην παράγραφο 3.12.1.).	Όπως περιγράφονται στην παράγραφο 3.12.2..	Όπως περιγράφονται στην παράγραφο 4.13..
	Πολλαπλασιασμός Εικονικών Μηχανών (VM Sprawl) (Όπως περιγράφονται στην παράγραφο 3.13.1.).	α. Ταχύτατος πολλαπλασιασμός εικονικών μηχανών με άγνωστη παραμετροποίηση και ρυθμίσεις. β. Άρνηση υπηρεσίας (DoS). γ. Υποβάθμιση της συνολικής απόδοσης του συστήματος. δ. Μη ύπαρξη αποτελεσματικού ελέγχου του συστήματος.	Όπως περιγράφονται στην παράγραφο 4.14..

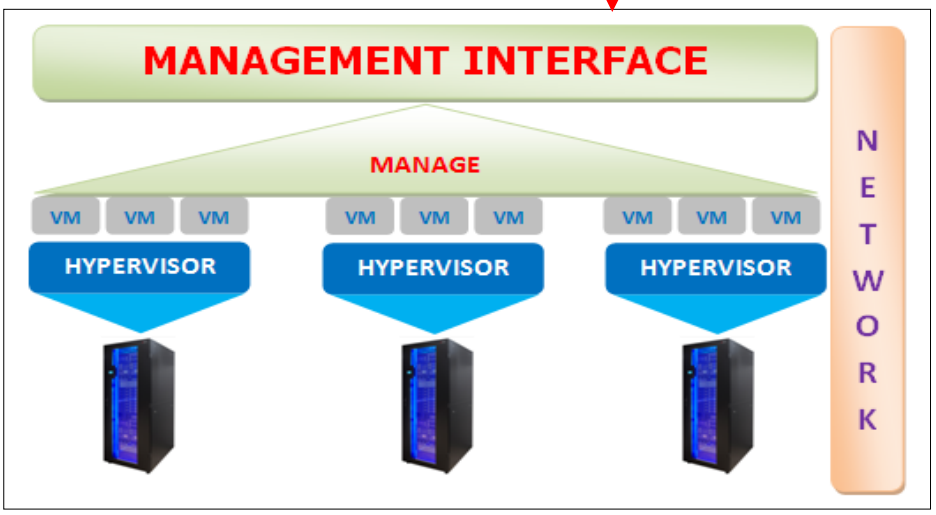
5

Ασφάλεια Αρχιτεκτονικής Εικονικοποίησης (Virtualization) Μέσω Εφαρμογής Καλών Πρακτικών

Η αρχιτεκτονική του υπολογιστικού νέφους (cloud computing) απεικονίζεται στην **Εικόνα 41**. Σε αυτό το Κεφάλαιο από όλα τα απεικονιζόμενα στρώματα των υπηρεσιών του υπολογιστικού νέφους θα ασχοληθούμε με αυτό της εικονικοποίησης (virtualization) και των τμημάτων που την απαρτίζουν, όπως αυτά απεικονίζονται στην **Εικόνα 42**. Ο στόχος είναι μέσω της εφαρμογής καλών πρακτικών ασφαλείας, για όλα τα μέρη που απαρτίζουν την εικονικοποίηση (virtualization), να οδηγηθούμε σε υψηλά επίπεδα ασφαλείας της αρχιτεκτονικής εικονικοποίησης (virtualization) της **Εικόνα 42**, στην οποία βασίζει την λειτουργία του μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing). Δεν θα επεκταθούμε καθόλου στην ασφάλεια του φυσικού υλικού και του λειτουργικού συστήματος του μηχανήματος υποδοχής (host operating system) καθώς αυτά είναι μέρος «συμβατικών» μέτρων προστασίας και «συμβατικών» καλών πρακτικών ασφαλείας. Προκειμένου, λοιπόν, να επιτύχουμε υψηλά επίπεδα ασφαλείας πρέπει να εφαρμόζονται με ιδιαίτερη προσοχή σε ένα σύστημα οι καλές πρακτικές που θα αναλυθούν σε αυτό το Κεφάλαιο και όλα τα μέτρα ασφαλείας που αναλύθηκαν στο Κεφάλαιο 4.



Εικόνα 41 - Αρχιτεκτονική Υπολογιστικού Νέφους (Cloud Computing) [83]



Εικόνα 42 - Αρχιτεκτονική Εικονικοποίησης (Virtualization) [41]

Η ασφάλεια της εικονικοποίησης (virtualization) εξαρτάται από την ασφάλεια όλων των μερών που την απαρτίζουν, τα οποία είναι ο hypervisor, η διεπαφή διαχείριση (management interface), οι εικονικές μηχανές (virtual machines) και το εικονικό δίκτυο επικοινωνίας (virtual network), όπως αυτά απεικονίζονται στην **Εικόνα 42**. Επομένως, οι οργανισμοί πρέπει να ασφαλίσουν και να διατηρήσουν την ασφάλεια όλων αυτών των στοιχείων με την χρήση καλών πρακτικών ασφαλείας. Στις ενότητες 5.1., 5.2., 5.3. και 5.4. που ακολουθούν θα αναλύσουμε τις καλές πρακτικές που πρέπει να εφαρμόζονται για την ασφάλεια των hypervisor, διεπαφής διαχείρισης (management interface), εικονικών μηχανών (virtual machines) και εικονικού

δικτύου επικοινωνίας (virtual network) αντίστοιχα. Τέτοιες πρακτικές είναι ο περιορισμός της πρόσβασης στις διεπαφές διαχείρισης, η διατήρηση του λογισμικού ενημερωμένου με τις τελευταίες διορθώσεις ασφαλείας, η χρήση σωστών πρακτικών διαμόρφωσης, η παρακολούθηση και η ανάλυση των αρχείων καταγραφής και η χρήση τείχων προστασίας, λογισμικού προστασίας από ιούς και άλλων κατάλληλων μηχανισμών για τον εντοπισμό και την αποτροπή των επιθέσεων. Σε γενικές γραμμές θα πρέπει να ακολουθούνται οι ίδιοι έλεγχοι ασφαλείας τόσο για τα λειτουργικά συστήματα των εικονικών μηχανών (virtual machines) όσο και γι αυτά που εγκαθίστανται απευθείας πάνω στο υλικό (hardware) **[12]**.

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους (cloud computing) είναι οι κύριοι υπεύθυνοι για την εφαρμογή των καλών πρακτικών καθώς αυτοί παρέχουν την υποδομή στους πελάτες – χρήστες των υπηρεσιών. Η πρωταρχική ευθύνη των παρόχων είναι η δημιουργία ενός ασφαλούς και απομονωμένου περιβάλλοντος για κάθε χρήστη. Κάθε χρήστης της υπηρεσίας πρέπει να έχει πρόσβαση στο δικό του και μόνο περιβάλλον εργασίας και σε καμία περίπτωση σε περιβάλλον εργασίας οποιουδήποτε άλλου χρήστη. Κανένας χρήστης δεν πρέπει να έχει πρόσβαση στα δεδομένα, στο σύστημα και σε οποιοδήποτε άλλο χαρακτηριστικό του περιβάλλοντος εργασίας άλλου χρήστη **[30]**.

5.1. Καλές Πρακτικές Ασφάλειας του Hypervisor ή VMM

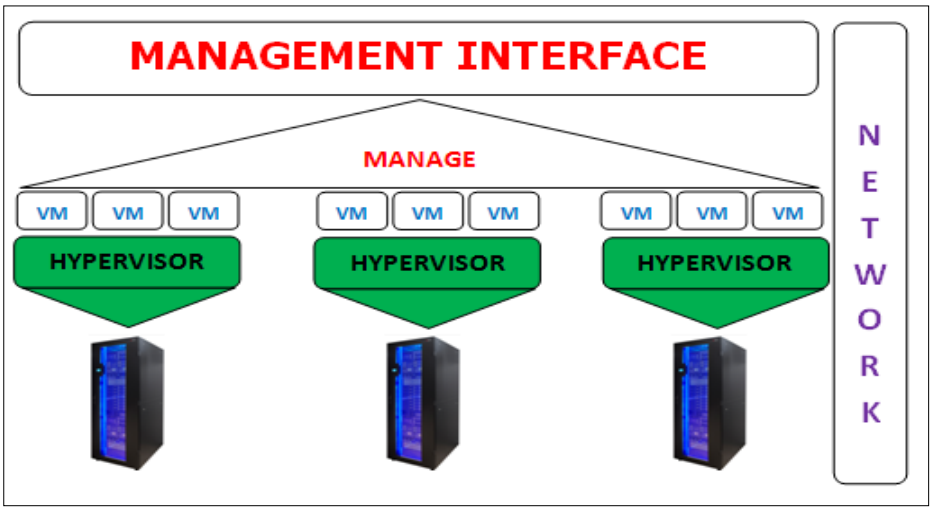
Σε ένα σύστημα θα πρέπει να εφαρμόζονται όλες οι τεχνικές απομόνωσης, οι οποίες συμβάλουν στη ασφαλή απομόνωση των εικονικών μηχανών (virtual machines) μεταξύ τους και λειτουργούν κάτω από τον έλεγχο του hypervisor. Οι τεχνικές αυτές είναι η απομόνωση εντολών (ανατρέξτε στην ενότητα 2.2.5. για λεπτομέρειες), η απομόνωση μνήμης (ανατρέξτε στην ενότητα 2.2.6.5. για λεπτομέρειες), η απομόνωση δικτύου (ανατρέξτε στην ενότητα 2.2.6.3. για λεπτομέρειες) και η απομόνωση συσκευών καθώς επίσης και η ορθή διαχείριση των φυσικών πόρων **[31]**.

Για να προστατεύσουμε τον hypervisor, ο οποίος απεικονίζεται με πράσινο φόντο στην αρχιτεκτονική εικονικοποίησης (virtualization) της **Εικόνα 43**, από απειλές κατά της ασφάλειας του θα πρέπει να επιβληθούν περιορισμοί σε παραμέτρους, ρυθμίσεις και δραστηριότητες αυτού. Κάτι τέτοιο, λοιπόν, μπορούμε να το επιτύχουμε με την εφαρμογή των καλών πρακτικών ασφαλείας του hypervisor, οι οποίες είναι:

- Σε περίπτωση ενεργοποίησης της απομακρυσμένη πρόσβαση στον hypervisor θα πρέπει η πρόσβαση να γίνεται μέσω ασφαλούς σύνδεσης δικτύου και με χρήση αυθεντικοποίησης με δυο διαφορετικούς τρόπους (2-factor authentication). Επιπροσθέτως, θα πρέπει να οριστούν και πολιτικές διαχείρισης συνεδρίας (session), προκειμένου να τερματίζονται παραδείγματος χάριν αδρανείς ή ανενεργές συνδέσεις, για να αποτραπεί οποιαδήποτε ενδεχόμενο παραβίασης.
- Οι ανοιχτές πόρτες του τείχους προστασίας πρέπει να είναι μόνο αυτές που απαιτούνται για την σωστή λειτουργία των εφαρμογών και υπηρεσιών.
- Στον hypervisor πρέπει να είναι σε λειτουργία μόνο οι απαραίτητες υπηρεσίες για την διαχείριση των λειτουργιών του.
- Χρήση πρωτοκόλλων κρυπτογράφησης δικτύου, όπως Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS), IPsec και άλλα πρωτόκολλα ασφαλούς επικοινωνίας καθώς και χρήση ισχυρών αλγόριθμων κρυπτογράφησης και διαχείρισης κλειδιών (ανατρέξτε στην ενότητα 4.1.4.1. για λεπτομέρειες).
- Παρακολούθηση όλων των προειδοποιήσεων ασφαλείας που θα μπορούσαν να επηρεάσουν την ασφάλεια του hypervisor και άμεση εφαρμογή διορθώσεων ασφαλείας. Επιπλέον, εγγραφή για λήψη όλων των ειδοποιήσεων και δελτίων ενημέρωσης ασφαλείας του παρόχου λογισμικού εικονικοποίησης (virtualization) και άμεση εφαρμογή όλων των ενημερώσεων (updates).
- Αποφυγή της χρήση μη ασφαλών υπηρεσιών όπως παραδείγματος χάριν FTP και Telnet.
- Επιλογή τύπου 1 hypervisor αντί για τύπου 2 (ανατρέξτε στην ενότητα 2.2.2. για λεπτομέρειες) καθώς έχει μικρότερο αποτύπωμα (footprint)

με αποτέλεσμα την μείωση της επιφάνειας επίθεσης (attack surface) και κατ᾽ επέκταση την εμφάνιση λιγότερων ευπαθειών.

- Αποσύνδεση όλων των φυσικών συσκευών υλικού που δεν χρησιμοποιούνται καθώς και απενεργοποίηση του clipboard και της κοινής χρήσης αρχείων.
- Διενέργεια ελέγχου αυτό-ακεραιότητας (self-integrity checks) κατά την εκκίνηση (boot-up) για επιβεβαίωση αν έχει παραβιαστεί ή όχι ο hypervisor, με χρήση ανάλογης τεχνολογίας παρακολούθησης της ακεραιότητας του, όπως παραδείγματος χάριν Intel Trusted Platform Module/Trusted Execution Technology.
- Ανάλυση και έλεγχο των αρχείων καταγραφής (logs) του hypervisor για εντοπισμό πιθανών ενδείξεων που τον θέτουν σε κίνδυνο.
- Εφαρμογή αποτελεσματικού μηχανισμού ελέγχου πρόσβασης (ACM) και ελέγχου ταυτότητας σε όλα τα εργαλεία και εφαρμογές, τα οποία καλούν τον hypervisor μέσω διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces (APIs)).
- Περιορισμός στο ελάχιστο του αριθμού των λογαριασμών, οι οποίοι απαιτούν άμεση πρόσβαση στον hypervisor.
- Ορθή διαχείριση και έλεγχος της κατανομής των πόρων στις εικονικές μηχανές (virtual machines) **[11]**, **[32]**.



Εικόνα 43 - Θέση Hypervisor στην Αρχιτεκτονική Εικονικοποίησης

5.2. Καλές Πρακτικές Ασφάλειας της Διεπαφής Διαχείρισης (Management Interface)

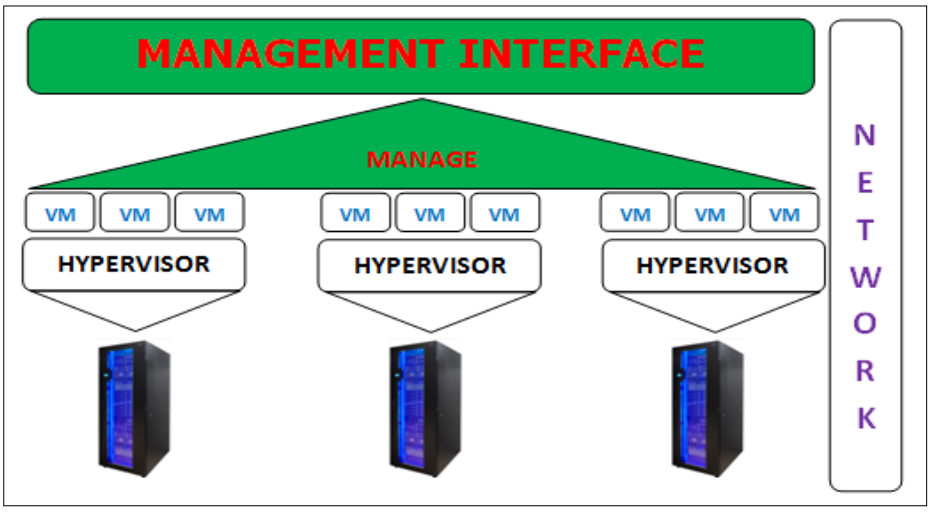
Σε ένα περιβάλλον εικονικοποίησης (virtualization) όλες οι υπηρεσίες που συνδέονται με την διεπαφή διαχείρισης, η οποία απεικονίζεται με πράσινο φόντο στην αρχιτεκτονική εικονικοποίησης (virtualization) της **Εικόνα 44**, πρέπει να προστατεύονται αποτελεσματικά. Αρχικά λοιπόν πρέπει να εφαρμόσουμε μέτρα ενδυνάμωσης ασφαλείας σε κάθε υπολογιστική μηχανή μέσα στην οποία «τρέχει» η διεπαφή διαχείρισης. Τα μέτρα ενδυνάμωσης ασφαλείας περιγράφονται στον **Πίνακας 1**, ως ασφάλεια λειτουργικού συστήματος μηχανήματος υποδοχής (host operating system).

Επιπλέον, πρέπει να εφαρμόζονται σωστές διαδικασίες ανάθεσης ρόλων και δικαιωμάτων σε χρήστες και ομάδες, το οποίο θα συμβάλει στην καλύτερη διαχείριση του περιβάλλοντος εικονικοποίησης (virtualization). Μέσα σε αυτό το πλαίσιο, λοιπόν, θα πρέπει να εκχωρούνται δικαιώματα μόνο στα αντικείμενα που τα χρειάζονται και προνόμια σε χρήστες ή ομάδες που πρέπει να τα έχουν. Με την ανάθεση του ελάχιστου αριθμού δικαιωμάτων γίνεται ευκολότερη και η δομή της διαχείριση τους. Τέλος, πρέπει να υπάρχει περιορισμός των δικαιωμάτων των διαχειριστών αναλόγως του ρόλου που τους έχει ανατεθεί και πρέπει να αποφεύγεται η χρήση ανώνυμων διαχειριστών.

Η εγκατάσταση Network Time Protocol (NTP) για τον συγχρονισμό των ρολογιών όλων των κόμβων που συμμετέχουν στο δίκτυο διαχείρισης κρίνεται αναγκαία. Αν τα ρολόγια όλων των μηχανών του δικτύου διαχείρισης δεν είναι συγχρονισμένα ενδέχεται τα πιστοποιητικά Secure Socket Layer (SSL), τα οποία είναι ευαίσθητα στον παράγοντα χρόνο, να μην αναγνωρίζονται ως έγκυρα κατά την διάρκεια της επικοινωνίας μεταξύ των μηχανών του δικτύου και να οδηγήσουν σε προβλήματα αυθεντικοποίησης.

Τέλος, οι καλές πρακτικές ασφαλείας του ελέγχου πρόσβασης της διεπαφής διαχείρισης με σκοπό να αποτραπεί οποιαδήποτε ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης είναι:

- Εφαρμογή μηχανισμού ασφαλείας ελέγχου πρόσβασης βάση ρόλων (Role Based Access Control (RBAC)) για όλες τις δραστηριότητες διαχείρισης της διεπαφής διαχείρισης (ανατρέξτε στην ενότητα 4.1.4.5. για λεπτομέρειες).
- Όλες οι δραστηριότητες διαχείρισης πρέπει να ελέγχονται από περισσότερα του ενός ατόμων για μεγαλύτερο, ασφαλέστερο και αποτελεσματικότερο έλεγχο και εποπτεία.
- Εάν ο τοπικός λογαριασμός διαχειριστή έχει πλήρη δικαιώματα διαχείρισης στην διεπαφή διαχείρισης πρέπει να αφαιρεθούν και να μοιραστούν σε περισσότερους του ενός λογαριασμούς διαχειριστών. Πλήρη δικαιώματα πρέπει να δίνονται μόνο σε διαχειριστές οι οποίοι με βάση τον ρόλο τους υποχρεούνται να τα έχουν.
- Περιορισμό της πρόσβασης στην διεπαφή διαχείρισης και απενεργοποίηση των διεπαφών που δεν χρησιμοποιούνται. Η πρόσβαση πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες και όλες οι ενέργειες πρέπει να καταγράφονται και να ελέγχονται. Επιπλέον, το τείχος προστασίας πρέπει να απαγορεύει την πρόσβαση από μη αξιόπιστες περιοχές.
- Περιορισμός, καταγραφή και έλεγχος των ενεργειών και των δικαιωμάτων που παραχωρούνται στους διαχειριστές των βάσεων δεδομένων.
- Ύπαρξη πολιτικής κωδικού πρόσβασης **[32]**.



Εικόνα 44 - Θέση Διεπαφής Διαχείρισης στην Αρχιτεκτονική Εικονικοποίησης

5.3. Καλές Πρακτικές Ασφάλειας των Εικονικών Μηχανών (Virtual Machines)

Οι καλές πρακτικές ασφαλείας που εφαρμόζονται για τις φυσικές μηχανές ισχύουν σε γενικές γραμμές και για τις εικονικές μηχανές (virtual machines), οι οποίες απεικονίζονται με πράσινο φόντο στην αρχιτεκτονική εικονικοποίησης (virtualization) της **Εικόνα 45**. Ωστόσο, αναφορικά με τις εικονικές μηχανές (virtual machines) ισχύουν και κάποιες επιπλέον καλές πρακτικές ασφαλείας λόγω της λειτουργίας τους μέσα σε περιβάλλον εικονικοποίησης (virtualization). Οι καλές πρακτικές ασφαλείας των εικονικών μηχανών (virtual machines) ταξινομούνται σε τέσσερις κατηγορίες, οι οποίες είναι:

1. Γενικά μέτρα προστασίας εικονικών μηχανών (virtual machines).
2. Χρήση προτύπων για την δημιουργία εικονικών μηχανών (virtual machines).
3. Αποτροπή εικονικών μηχανών (virtual machines) από την χρήση περισσότερων πόρων από αυτές που τους έχουν ανατεθεί.
4. Απενεργοποίηση περιττών λειτουργιών μέσα στις εικονικές μηχανές (virtual machines).

5.3.1. Γενικά Μέτρα Προστασίας Εικονικών Μηχανών (Virtual Machines)

Τα γενικά μέτρα προστασίας των εικονικών μηχανών (virtual machines) είναι τα ίδια με αυτά που ισχύουν και για τις φυσικές μηχανές. Επομένως, τα γενικά μέτρα προστασίας των εικονικών μηχανών (virtual machines) είναι:

- Ενημέρωση του λογισμικού των εικονικών μηχανών (virtual machines) με τις τελευταίες ενημερώσεις και διορθώσεις ασφαλείας. Ιδιαίτερη προσοχή θα πρέπει να δίνεται στην ενημέρωση των αδρανών (dormant), εκτός λειτουργίας (offline) και εικονικών μηχανών (virtual machine) που έχουν επαναφερθεί σε προηγούμενη καλή κατάσταση λειτουργίας.

- Εγκατάσταση σε κάθε εικονική μηχανή (virtual machine) λογισμικού προστασίας από ιούς (anti-virus) και λειτουργία τείχους προστασίας (firewall). Επιπλέον, αναλόγως της χρήσης κάθε εικονικής μηχανής (virtual machine) μπορεί να χρήζει εγκατάσταση και επιπλέον μηχανισμών ασφαλείας.
- Ύπαρξη χρονοδιαγράμματος λειτουργίας σάρωσης από ιούς, ιδιαίτερα σε αναπτύξεις με μεγάλο αριθμό εικονικών μηχανών (virtual machines) καθώς η απόδοση των συστημάτων θα υποβαθμιστεί σημαντικά σε περίπτωση λειτουργίας σάρωσης των εικονικών μηχανών (virtual machines) ταυτόχρονα.
- Επιβεβαίωση ότι όλοι οι μηχανισμοί ασφαλείας όπως λογισμικό προστασίας από ιούς (anti-virus), anti-spyware, σύστημα ανίχνευσης και αποτροπής εισβολών (IDPS) και άλλοι είναι σε λειτουργία για κάθε εικονική μηχανή (virtual machine) του περιβάλλοντος εικονικοποίησης (virtualization).
- Επιβεβαίωση ότι υπάρχει αρκετός αποθηκευτικός χώρος για τα αρχεία καταγραφής της εικονικής μηχανής (virtual machine).

5.3.2. Χρήση Προτύπων για την Δημιουργία Εικονικών Μηχανών (Virtual Machines)

Η χρήση προτύπων στην δημιουργία νέων εικονικών μηχανών (virtual machines) είναι σημαντική καθώς στα πρότυπα είναι εγκατεστημένα λειτουργικά συστήματα που τηρούν όλα τα μέτρα ενδυνάμωσης (ανατρέξτε στον **Πίνακας 1** για λεπτομέρειες) και προστασίας (ανατρέξτε στην ενότητα 5.3.1. για λεπτομέρειες) των λειτουργικών συστημάτων. Με αυτό τον τρόπο εξαλείφεται ο κίνδυνος δημιουργίας εικονικής μηχανής (virtual machine) με λάθη παραμετροποίησης, γίνεται εξοικονόμηση χρόνου καθώς εξαλείφεται η ανάγκη για εφαρμογή επαναλαμβανόμενων ρυθμίσεων σε κάθε νέα εικονική μηχανή (virtual machine) που δημιουργείται και επιπλέον εξασφαλίζουμε ότι όλες οι εικονικές μηχανές (virtual machines) ακολουθούν ένα γνωστό βασικό επίπεδο ασφαλείας. Τα πρότυπα αποθηκεύονται σε μορφή αρχείων γι αυτό είναι απαραίτητη η διασφάλισης της ακεραιότητας τους, η οποία μπορεί να

επιτευχθεί με την εφαρμογή όλων των μέτρων ασφαλείας του αναφέρονται στην ενότητα 4.7..

5.3.3. Αποτροπή Εικονικών Μηχανών (Virtual Machines) από την Χρήση Περισσότερων Πόρων από Αυτούς που τους Έχουν Ανατεθεί

Για να αποτρέψουμε μια εικονική μηχανή (virtual machine) να κάνει χρήση περισσότερων πόρων από ότι οι υπόλοιπες εικονικές μηχανές (virtual machines) πρέπει να κάνουμε χρήση όλων των λειτουργιών διαχείρισης πόρων όπως είναι οι ρυθμίσεις διαμοιρασμού πόρων και η δημιουργία δεξαμενών πόρων (resource pools). Έτσι λοιπόν πρέπει:

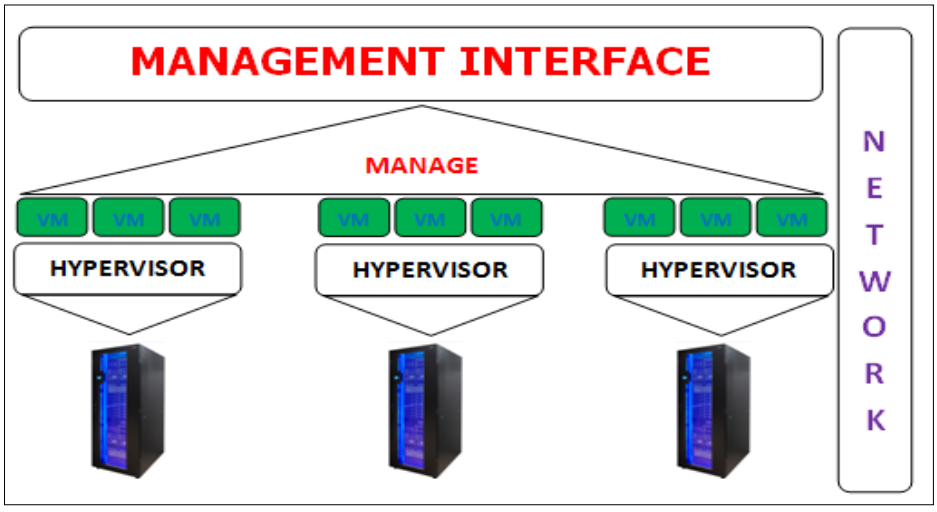
- Να παρέχουμε τους απαραίτητους πόρους σε κάθε εικονική μηχανή (virtual machine) για την ορθή λειτουργίας της.
- Να ομαδοποιήσουμε τις εικονικές μηχανές (virtual machines) με βάση τις απαιτήσεις τους σε πόρους για την δημιουργία ανάλογων δεξαμενών πόρων (resource pools).
- Να ορίσουμε ίδιες προτεραιότητες πρόσβασης στους πόρους για όλες τις εικονικές μηχανές (virtual machines) που συμμετέχουν σε κάθε δεξαμενή πόρων (resource pools).
- Να υπάρχει παρακολούθηση και έλεγχος στην κατανομή και στην εξάντληση των πόρων.

5.3.4. Απενεργοποίηση Περιττών Λειτουργιών Μέσα στις Εικονικές Μηχανές (Virtual Machines)

Κάθε υπηρεσία που εκτελείται μέσα σε μία εικονική μηχανή (virtual machine) μπορεί να γίνει στόχος επίθεσης. Με την απενεργοποίηση

εξαρτημάτων ή λειτουργιών που δεν είναι πλέον αναγκαία μειώνεται ταυτόχρονα και η επιφάνεια επίθεσης. Έτσι λοιπόν πρέπει:

- Να απενεργοποιούνται υπηρεσίες των λειτουργικών συστημάτων που δεν χρησιμοποιούνται, όπως παραδείγματος χάριν εάν θέσουμε σε λειτουργία μέσα σε μία εικονική μηχανή έναν διακομιστή αρχείων να απενεργοποιήσουμε όλες τις υπηρεσίας του διαδικτύου (Web services).
- Να αποσυνδέονται όλες οι φυσικές συσκευές που δεν χρησιμοποιούνται, όπως παραδείγματος χάριν οδηγοί CD/DVD, μονάδες δισκέτας και προσαρμογείς USB.
- Να απενεργοποιούνται λειτουργίες που δεν χρησιμοποιούνται, όπως παραδείγματος χάριν χαρακτηριστικά οθόνης που δεν χρησιμοποιούνται και διαμοιραζόμενοι φάκελοι και αρχεία μεταξύ των εικονικών μηχανών (virtual machines) και του μηχανήματος υποδοχής (host machine).
- Να γίνεται διαγραφή οδηγών (drivers) και λογισμικού που δεν χρησιμοποιείται.
- Να εγκαθίσταται βοηθητικό λογισμικό μόνο αν χρειάζεται.
- Να απενεργοποιείται ή να διαγράφεται το εικονικό υλικό που δεν χρησιμοποιείται, όπως K.M.E, RAM, οδηγοί πολυμέσων, προσαρμογείς δικτύων και άλλα **[32]**.

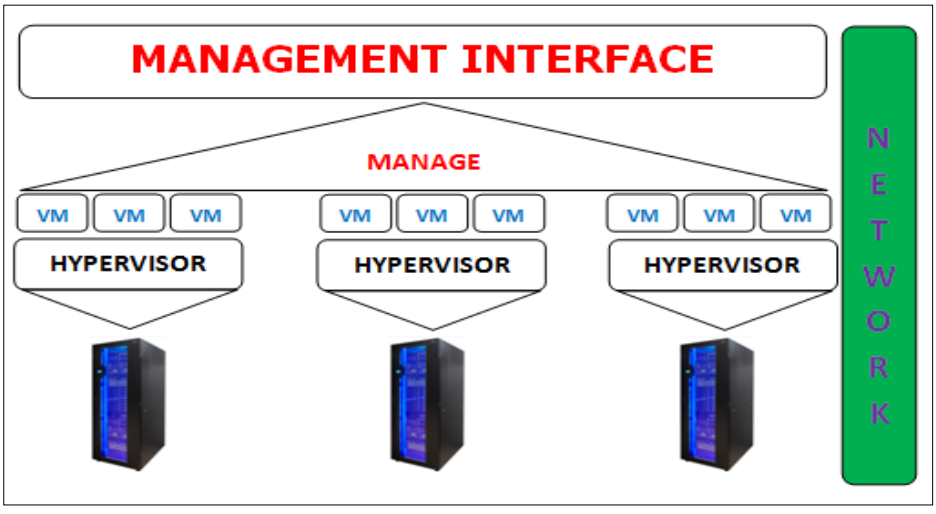


Εικόνα 45 - Θέση Εικονικών Μηχανών στην Αρχιτεκτονική Εικονικοποίησης

5.4. Καλές Πρακτικές Ασφάλειας του Εικονικού Δικτύου (Virtual Network)

Το εικονικό δίκτυο (virtual network) περιλαμβάνει προσαρμογείς δικτύου (network adapters), εικονικούς μεταγωγείς (virtual switches), κατανεμημένους εικονικούς μεταγωγείς (distributed virtual switches), πόρτες (ports) και ομάδες πορτών (port groups) για την επικοινωνία όλων των μερών της εικονικοποίησης (virtualization) και απεικονίζεται με πράσινο φόντο στην αρχιτεκτονική εικονικοποίησης (virtualization) της **Εικόνα 46**. Κάθε στοιχείο της υποδομής του δικτύου θα πρέπει να μπορεί να ασφαλιστεί χωριστά. Ο hypervisor στηρίζεται στο εικονικό δίκτυο για την υλοποίηση της επικοινωνίας μεταξύ των εικονικών μηχανών (virtual machines) και των χρηστών αυτών. Επιπλέον, ο hypervisor χρησιμοποιεί το εικονικό δίκτυο για να επικοινωνήσει με τις διεπαφές αποθήκευσης, όπως παραδείγματος χάριν iSCSI SANs και NAS **[31]**. Οι καλές πρακτικές ασφαλείας του δικτύου ταξινομούνται σε τέσσερις κατηγορίες, οι οποίες είναι:

1. Απομόνωση δικτυακής κίνησης.
2. Χρήση τείχων προστασίας (firewalls) για την ασφάλεια όλων των στοιχείων του εικονικού δικτύου.
3. Ύπαρξη πολιτικής ασφαλείας δικτύου.
4. Δημιουργία VLANs για προστασία του περιβάλλοντος εικονικοποίησης (virtualization).



Εικόνα 46 - Θέση Εικονικού Δικτύου στην Αρχιτεκτονική Εικονικοποίησης

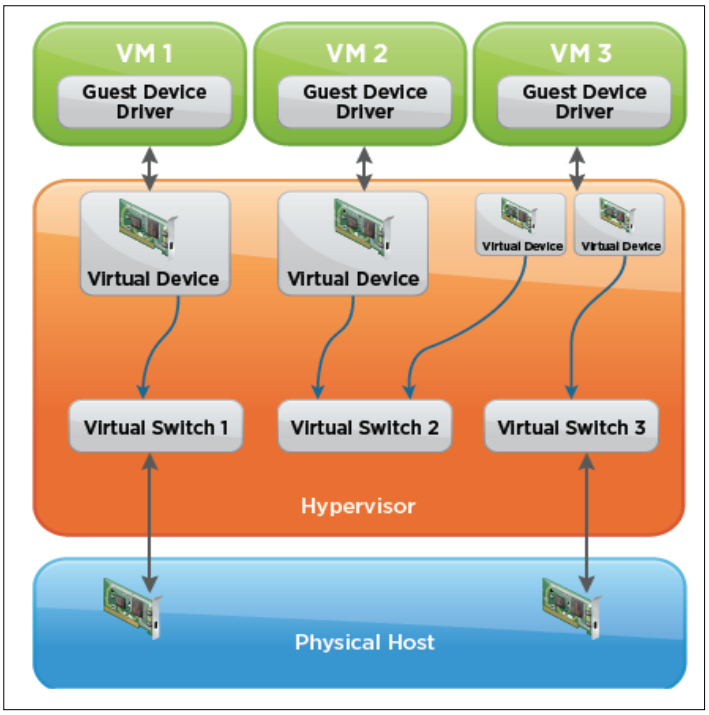
5.4.1. Απομόνωση Δικτυακής Κίνησης

Η απομόνωση της δικτυακής κίνησης είναι απαραίτητη για την δημιουργία ενός ασφαλούς περιβάλλοντος εικονικοποίησης (virtualization). Διαφορετικά δίκτυα απαιτούν διαφορετική πρόσβαση και διαφορετικό επίπεδο απομόνωσης. Στην **Εικόνα 47** απεικονίζεται ένα διάγραμμα αυξημένου επιπέδου ευαισθησίας των εικονικών δικτύων σε ένα περιβάλλον εικονικοποίησης (virtualization), στο οποίο το επίπεδο ευαισθησίας αυξάνει από το εξωτερικό επίπεδο προς το εσωτερικό. Επιπλέον, από την **Εικόνα 47** προκύπτει η ανάγκη της απομόνωσης της δικτυακής κυκλοφορίας για συγκεκριμένες εφαρμογές και λειτουργίες. Για παράδειγμα θα πρέπει να απομονώσουμε το δίκτυο διαχείρισης από το δίκτυο επικοινωνίας των εικονικών μηχανών (virtual machines) και για λόγους καλύτερης απόδοσης αυτών άλλα και για να αποτρέψουμε την υποκλοπή της κίνησης του ενός δικτύου από το άλλο.

Εικόνα 47 - Διάγραμμα Αυξημένου Επιπέδου Ευαισθησίας Εικονικών Δικτύων [31]

Ακολουθεί σύντομη περιγραφή των απαιτούμενων εικονικών δικτύων μέσα σε ένα σύστημα υπολογιστικού νέφους (cloud computing system), τα οποία πρέπει να είναι απομονωμένα το ένα από το άλλο:

- Δίκτυα υποδομής. Τα δίκτυα υποδομής χρησιμοποιούνται για λειτουργίες όπως μετανάστευσης εικονικών μηχανών (virtual machines), ανοχής σφαλμάτων και αποθήκευσης. Τα δίκτυα αυτά πρέπει να είναι απομονωμένα για συγκεκριμένες λειτουργίες τους και να μην δρομολογούνται, δηλαδή να μην υπάρχει δυνατότητα κάποιος από έξω να αποκτήσει πρόσβαση σε αυτά.
- Δίκτυο διαχείρισης. Το δίκτυο διαχείρισης απομονώνει την πρόσβαση των χρηστών στις εικονικές μηχανές (virtual machines), την κυκλοφορία των Command-Line Interfaces (CLIs) ή των Application Programming Interfaces (APIs) και την κυκλοφορία του λογισμικού των third-parties από την κανονική κυκλοφορία. Το δίκτυο πρέπει να είναι προσβάσιμο μόνο από το σύστημα και τους διαχειριστές ασφαλείας και για την ασφάλεια της πρόσβασης σε αυτό συνίσταται η χρήση "jump box" ή virtual private network (VPN).
- Δίκτυα εικονικών μηχανών (virtual machines). Τα δίκτυα εικονικών μηχανών (virtual machines) μέσω των οποίων διεξάγεται η επικοινωνία των εικονικών μηχανών (virtual machines) μπορεί να είναι ένα ή πολλαπλά. Η απομόνωση των εικονικών μηχανών (virtual machines) μέσα σε αυτά τα δίκτυα ενισχύεται με την χρήση εικονικών τείχων προστασίας, τα οποία ορίζουν κανόνες στους ελεγκτές εικονικών δικτύων. Όλες οι ρυθμίσεις δικτύου που πραγματοποιούνται σε μία εικονική μηχανή (virtual machine) πρέπει να την ακολουθούν κατά την διαδικασία μετανάστευσης της από το ένα μηχάνημα υποδοχής (host machine) στο άλλο, μέσα στο ίδιο cluster. Μία εικονική μηχανή (virtual machine) επικοινωνεί με άλλες εικονικές μηχανές (virtual machines) που λειτουργούν κάτω από τον ίδιο hypervisor μέσω ενός εικονικού μεταγωγέα (virtual switch) και επιπλέον επικοινωνεί με το φυσικό δίκτυο συμπεριλαμβανομένου και εικονικών μηχανών (virtual machines) που λειτουργούν κάτω από άλλους hypervisors μέσω ενός φυσικού προσαρμογέα δικτύου (physical network adapter). Ένα παράδειγμα απομόνωσης εικονικών μηχανών (virtual machines) φαίνεται στην **Εικόνα 48**.



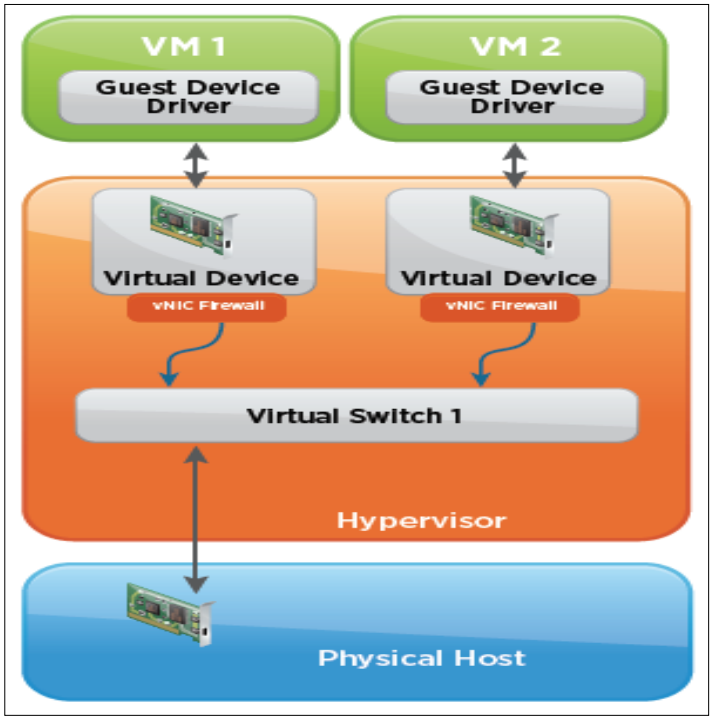
Εικόνα 48 - Παράδειγμα Απομόνωσης Εικονικών Μηχανών [31]

Με βάση την **Εικόνα 48**:

- Εάν μία εικονική μηχανή (virtual machine) δεν μοιράζεται έναν εικονικό μεταγωγέα (virtual switch) με καμία άλλη εικονική μηχανή (virtual machine) μέσα στον ίδιο hypervisor είναι εντελώς απομονωμένη από τα άλλα εικονικά δίκτυα. Αυτή είναι η VM 1 της **Εικόνα 48**.
- Εάν δεν έχει ρυθμιστεί φυσικός προσαρμογέας δικτύου για μία εικονική μηχανή (virtual machine), αυτή είναι εντελώς απομονωμένη από οποιοδήποτε φυσικό δίκτυο. Αυτή είναι η VM 2 της **Εικόνα 48**. Σε αυτή την περίπτωση, η πρόσβαση σε ένα φυσικό δίκτυο μπορεί να επιτευχθεί εάν η VM 3 λειτουργεί ως δρομολογητής μεταξύ του εικονικού μεταγωγέα (virtual switch) 2 και του εικονικού μεταγωγέα (virtual switch) 3.
- Μια εικονική μηχανή (virtual machine) μπορεί να ρυθμιστεί από τον διαχειριστή να επικοινωνεί με δύο ή περισσότερους εικονικούς μεταγωγείς (virtual switch). Αυτή είναι η VM 3 της **Εικόνα 48**.

Όπως αναφέρθηκε παραπάνω, η απομόνωση των εικονικών μηχανών (virtual machines) μέσα σε ένα δίκτυο ενισχύεται με την χρήση εικονικών τειχων προστασίας, τα οποία ορίζουν κανόνες στους ελεγκτές εικονικών δικτύων. Με την χρήση, λοιπόν, τειχους προστασίας στο επίπεδο του ελεγκτή

εικονικού δικτύου (virtual network interface controller (vNIC)), μία εικονική μηχανή (virtual machine) μπορεί να απομονωθεί από τις άλλες εικονικές μηχανές (virtual machines) ακόμα και μέσα στον ίδιο εικονικό μεταγωγέα (virtual switch). Οι κανόνες του τείχους προστασίας εφαρμόζονται στον ελεγκτή εικονικού δικτύου (virtual network interface controller (vNIC)) και όχι στον εικονικό μεταγωγέα (virtual switch), όπως απεικονίζεται στην **Εικόνα 49**, **[31]**.



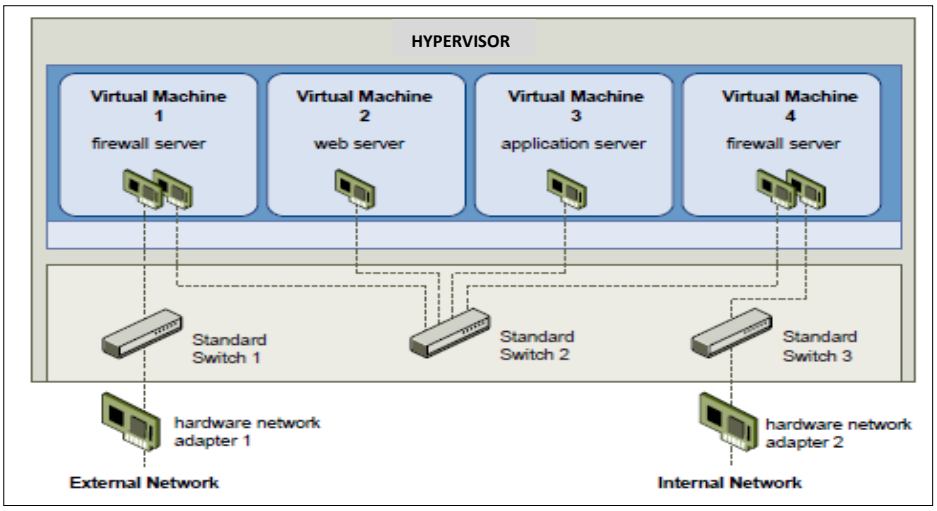
Εικόνα 49 - Παράδειγμα Εφαρμογής Κανόνων Τείχους Προστασίας [31]

5.4.2. Χρήση Τείχων Προστασίας (Firewalls) για την Ασφάλεια όλων των Στοιχείων του Εικονικού Δικτύου

Με την χρήση τείχους προστασίας σε ένα δίκτυο έχουμε την δυνατότητα να ανοίξουμε και να κλείσουμε πόρτες (ports) καθώς επίσης και να ασφαλίσουμε κάθε στοιχείο του εικονικού δικτύου χωριστά. Οι περιοχές που πρέπει να ενεργεί ένα τείχους προστασίας μέσα σε ένα εικονικό δίκτυο είναι:

- Εάν οι χρήστες έχουν πρόσβαση στις εικονικές μηχανές (virtual machines) μέσω ενός προγράμματος περιήγησης ιστού, ανάμεσα στο πρόγραμμα περιήγησης και στον hypervisor.
- Μεταξύ του δικτύου διαχείρισης και του hypervisor.
- Αν η πρόσβαση στο δίκτυο διαχείρισης γίνεται μέσω ενός προγράμματος περιήγησης ιστού, ανάμεσα στο πρόγραμμα περιήγησης και στο δίκτυο διαχείρισης.
- Αν στο δίκτυο υπάρχουν περισσότεροι του ενός hypervisors εγκατεστημένοι σε αντίστοιχα μηχανήματα υποδοχής (host machines), μεταξύ των hypervisors. Αν τοποθετηθούν τείχη προστασίας μεταξύ των διαφορετικών hypervisors ενός δικτύου τότε για να ενεργοποιήσουμε τις λειτουργίες της μετανάστευσης εικονικών μηχανών (virtual machines) μεταξύ των μηχανημάτων υποδοχής (host machines) και της εκτέλεση κλωνοποίησης εικονικών μηχανών (virtual machines) πρέπει να ανοίξουμε τις ανάλογες πόρτες στα τείχη προστασίας των μηχανημάτων υποδοχής (host machines) πηγής και προορισμού.
- Μεταξύ του hypervisor και του δικτύου αποθήκευσης.

Επιπλέον, το τείχος προστασίας ενισχύει την ασφάλεια του περιβάλλοντος εικονικοποίησης (virtualization) καθώς δίνει την δυνατότητα δημιουργίας αποστρατικοποιημένων ζωνών δικτύου (demilitarized zone (DMZ)) σε κάθε μηχάνημα υποδοχής (host machine). Ωστόσο, η ασφάλεια των εικονικών μηχανών (virtual machine) μέσα σε μία αποστρατικοποιημένη ζώνη δικτύου (demilitarized zone (DMZ)) πρέπει να αντιμετωπίζεται όπως όταν ξεχωριστές φυσικές μηχανές συνδέονται στο ίδιο δίκτυο, καθώς το δίκτυο μπορεί να χρησιμοποιηθεί για τον πολλαπλασιασμό ενός ιού ή άλλου είδους επιθέσεις. Ένα παράδειγμα δημιουργίας μιας αποστρατικοποιημένης ζώνης δικτύου (demilitarized zone (DMZ)) απεικονίζεται στην **Εικόνα 50**.



Εικόνα 50 - Παράδειγμα Δημιουργίας Αποστρατικοποιημένης Ζώνης (Demilitarized Zone (DMZ)) [32]

Σε αυτό το παράδειγμα οι τέσσερις εικονικές μηχανές (virtual machines) έχουν ρυθμιστεί με τέτοιο τρόπο ώστε να δημιουργήσουν μία εικονική αποστρατικοποιημένη ζώνη (demilitarized zone (DMZ)) στο Standard Switch 2. Για να γίνει αυτό, οι Virtual Machine 1 και Virtual Machine 4 «τρέχουν» τείχη προστασίας και συνδέονται με τους φυσικούς προσαρμογείς δικτύου μέσω των Standard Switch 1 και Standard Switch 3 αντίστοιχα και επιπλέον οι δυο αυτές εικονικές μηχανές (virtual machines) συνδέονται και με το Standard Switch 2. Επίσης, στην Virtual Machine 2 τρέχει ένας web server και στην Virtual Machine 3 τρέχει ένας application server και επιπλέον οι δυο αυτές εικονικές μηχανές (virtual machines) συνδέονται με το Standard Switch 2.

Ο web server και ο application server αποτελούν την αποστρατικοποιημένη ζώνη (demilitarized zone (DMZ)) μεταξύ των τείχων προστασίας. Ο δίαυλος επικοινωνίας μεταξύ αυτών είναι το Standard Switch 2, το οποίο συνδέει τα τείχη προστασίας με τους διακομιστές. Επιπλέον, το Standard Switch 2 δεν έχει άμεση επικοινωνία με κανένα στοιχείο που βρίσκεται έξω από την αποστρατικοποιημένη ζώνη (demilitarized zone (DMZ)) και είναι απομονωμένο από την εξωτερική κυκλοφορία των δύο τείχων προστασίας.

Από λειτουργικής πλευράς, η εξωτερική κίνηση του διαδικτύου δρομολογείται από το Standard Switch 1 στην Virtual Machine 1 μέσω του hardware network adapter 1 και επαληθεύεται από το τείχος προστασίας που

είναι εγκατεστημένο σε αυτή. Στην συνέχεια, αν το τείχος προστασίας επιτρέψει την περαιτέρω κυκλοφορία, αυτή στην συνέχεια δρομολογείται στο Standard Switch 2, το οποίο βρίσκεται μέσα στην αποστρατικοποιημένη ζώνη (demilitarized zone (DMZ)). Επειδή οι web server και application server είναι συνδεδεμένοι με το Standard Switch 2 μπορούν να εξυπηρετήσουν με αυτόν τον τρόπο εξωτερικές αιτήσεις. Επιπλέον, στο Standard Switch 2 είναι συνδεδεμένη και η Virtual Machine 4, στην οποία λειτουργεί τείχος προστασίας μεταξύ της αποστρατικοποιημένης ζώνης (demilitarized zone (DMZ)) και του εσωτερικού δικτύου. Επομένως, αυτό το τείχος προστασίας φιλτράρει τα πακέτα που προέρχονται από τους web server και application server προς το εσωτερικό δίκτυο. Κάθε πακέτο που επαληθεύεται δρομολογείται από το Standard Switch 3 στον hardware network adapter 2, ο οποίος συνδέεται με το εσωτερικό δίκτυο **[32]**.

5.4.3. Ύπαρξη Πολιτικής Ασφαλείας Δικτύου

Η πολιτική ασφαλείας δικτύου θα πρέπει να παρέχει τις απαραίτητες οδηγίες για την προστασία της δικτυακής κίνησης από επιθέσεις όπως πλαστοπροσωπία των διευθύνσεων Media Access Control (MAC) (ανατρέξτε στην ενότητα 3.10. για λεπτομέρειες) και port scanning (ανατρέξτε στην ενότητα 3.11. για λεπτομέρειες). Σε γενικότερο πλαίσιο θα πρέπει να παρέχει τις απαραίτητες οδηγίες για την ασφάλεια του εικονικού δικτύου και μέσω της πολιτικής θα πρέπει να επιβάλλεται:

- Η χρήση πρωτοκόλλων κρυπτογράφησης δικτύου, όπως Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS), IPsec και άλλα πρωτόκολλα ασφαλούς επικοινωνίας, τα οποία ενισχύουν την ασφάλεια αφού κρυπτογραφούν τα δεδομένα πριν την αποστολή τους και εφαρμόζουν μεθόδους αυθεντικοποίησης μόλις αυτά φτάσουν στον προορισμό τους.
- Η διεξαγωγή της παρακολούθησης των εικονικών δικτύων και της διαβίβασης των δεδομένων τους με πρακτικές που εφαρμόζονται στα φυσικά δίκτυα.

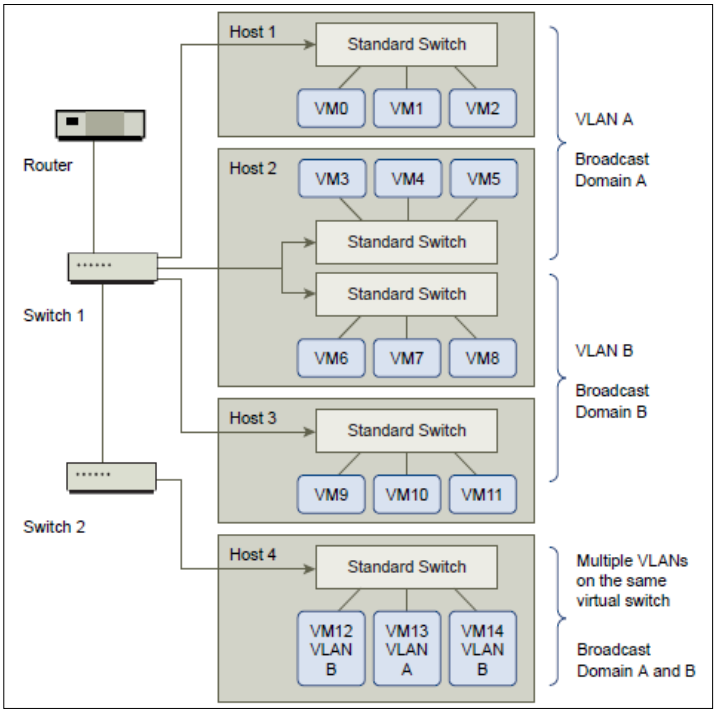
- Η χρήση τεχνολογιών ασφαλείας, όπως παραδείγματος χάριν εγκατάσταση και λειτουργία συστήματος ανίχνευσης και αποτροπής εισβολών (IDPS), οι οποίες πρέπει να λειτουργούν με τον ίδιο τρόπο τόσο στα φυσικά όσο και στα εικονικά περιβάλλοντα κάτω από το ίδιο πλαίσιο εφαρμογής και ακλουθώντας την ίδια πολιτική διαχείρισης.
- Η αποφυγή όσο είναι δυνατόν σχέσεων εμπιστοσύνης με την ανάπτυξη αντίστοιχων πρωτοκόλλων.
- Η ενσωμάτωση στις διεπαφές προγραμματισμού εφαρμογών (APIs) του hypervisor εξειδικευμένων μηχανισμών ασφαλείας εικονικών μηχανών (virtual machines) για την παροχή παρακολούθησης και ελέγχου της κυκλοφορίας των δεδομένων των εικονικών μηχανών (virtual machines) **[11]**, **[32]**.

5.4.4. Δημιουργία VLANs για Προστασία του Περιβάλλοντος Εικονικοποίησης (Virtualization)

Η χρήση VLANs μπορεί να ενισχύσει την ασφάλεια των εικονικών δικτύων καθώς το δίκτυο γενικότερα είναι ένα από τα πιο ευάλωτα τμήματα κάθε συστήματος. Τα VLANs είναι IEEE πρότυπα συστήματα δικτύωσης (IEEE standard networking scheme) με συγκεκριμένες μεθόδους σήμανσης και επιτρέπουν την δρομολόγηση των πακέτων μόνο σε εκείνες τις πόρτες (ports), οι οποίες αποτελούν μέρος του ίδιου VLAN. Εάν σε ένα εικονικό δίκτυο τα VLANs ρυθμιστούν σωστά παρέχουν ένα αξιόπιστο μέσο για την προστασία των επικοινωνούντων μερών του δικτύου από τυχαία ή «κακόβουλη» διείσδυση. Ουσιαστικά τα VLANs δεν επιτρέπουν σε δύο παραδείγματος χάριν εικονικές μηχανές (virtual machines) να μεταδώσουν πακέτα η μία στην άλλη αν δεν είναι μέρος του ίδιου VLAN.

Στην **Εικόνα 51** απεικονίζεται ένα παράδειγμα μίας διάταξης VLANs. Εάν ο δρομολογητής (Router) προωθεί πακέτα για τις εικονικές μηχανές (virtual machines) που ανήκουν στο VLAN A αυτά τα πακέτα θα έχουν σημανθεί για διανομή μόνο στο VLAN A. Με αυτό τον τρόπο τα πακέτα με την

συγκεκριμένη σήμανση περιορίζονται για μετάδοση μόνο στο Domain A και δεν μπορούν να μεταδοθούν στο Domain B, εκτός εάν γίνουν ανάλογες ρυθμίσεις στον δρομολογητή (Router). Επιπλέον, όπως φαίνεται και από την **Εικόνα 51**, οι εικονικές μηχανές (virtual machines) που ανήκουν σε κοινό μεταγωγέα δικτύου (virtual switch) μπορούν παράλληλα να ανήκουν σε διαφορετικά VLANs **[32]**.



Εικόνα 51 - Παράδειγμα Διάταξης VLANs [32]

6

Επίλογος

6.1. Σύνοψη – Συμπεράσματα

Σε αυτή την εργασία εξετάσαμε τον τρόπο εφαρμογής της εικονικοποίησης (virtualization) σε σύγχρονες αρχιτεκτονικές υπολογιστικών συστημάτων. Στην συνέχεια, μελετήσαμε τις ευπάθειες και τις απειλές που αντιμετωπίζει ένα σύστημα υπολογιστικού νέφους (cloud computing system) όταν εφαρμόζεται σε αυτό η τεχνολογία της εικονικοποίησης (virtualization) και παράλληλα αναλύσαμε τα μέτρα ασφαλείας για την αντιμετώπιση των ευπαθειών και απειλών της. Τέλος, παρουσιάσαμε τις καλές πρακτικές ασφαλείας όλων των μερών που απαρτίζουν την αρχιτεκτονική εικονικοποίησης (virtualization), στην οποία βασίζει την λειτουργία του μεγάλο μέρος των συστημάτων υπολογιστικού νέφους (cloud computing systems).

Η εικονικοποίηση (virtualization) προσφέρει πολλά πλεονεκτήματα σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) καθώς συμβάλει στην αποσύνδεση μεταξύ της λογικής και της φυσικής κατάστασης του υλικού μοιράζοντας παράλληλα τους φυσικούς πόρους σε πολλαπλά απομονωμένα μεταξύ τους περιβάλλοντα εκτέλεσης. Με την εικονικοποίηση (virtualization) μπορούμε, λοιπόν, να πετύχουμε μείωση του κόστους συντήρησης του υλικού και του κόστους κατανάλωσης ενέργειας, αποδοτικότερη χρήση του υλικού, οικονομία στην χρήση των πόρων, αποτελεσματικότερη διαχείριση, ευελιξία, επεκτασιμότητα και ασφάλεια.

Από την άλλη πλευρά όμως, ο σχεδιασμός, η υλοποίηση και η ανάπτυξη της συγκεκριμένης τεχνολογίας έχει εισάγει νέες προκλήσεις ασφαλείας. Η λειτουργία του hypervisor μέσα σε περιβάλλοντα εικονικοποίησης (virtualization) αποτελεί ένα μοναδικό σημείο αποτυχίας (single point of failure), καθώς αν ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση στον hypervisor θέτει την ασφάλεια του συστήματος σε κίνδυνο. Επιπλέον, αν δεν υπάρχουν κατάλληλες πολιτικές και διαδικασίες δημιουργίας, ασφαλείας, διανομής, αποθήκευσης, χρήσης, θέσεως εκτός ενεργείας και καταστροφής των εικονικών μηχανών (virtual machines) και των εικόνων (images) τους η πιθανότητα παραβίασης της ασφάλειας τους είναι πολύ μεγάλη.

Η εικονικοποίηση (virtualization), λοιπόν, έχει ευπάθειες και κατ΄ επέκταση απειλές, τις οποίες αναλύσαμε, με αποτέλεσμα να εισάγει ένα πρόσθετο επίπεδο κινδύνου στα συστήματα υπολογιστικού νέφους (cloud computing systems). Προκειμένου να εξαλείψουμε τις ευπάθειες και απειλές της εικονικοποίησης (virtualization) και να εκμεταλλευτούμε τα πλεονεκτήματα της, πρέπει η εφαρμογή της σε ένα σύστημα υπολογιστικού νέφους (cloud computing system) να γίνεται με μεγάλη προσοχή ακολουθώντας όλα τα μέτρα ασφαλείας και τις καλές πρακτικές ασφαλείας που αναλύθηκαν.

6.2. Μελλοντική Εργασία

Σε αυτή την εργασία αναλύσαμε τον τρόπο υλοποίησης της εικονικοποίησης (virtualization) με την τεχνική hardware virtualization, στην οποία κυρίαρχο ρόλο παίζει ο hypervisor, και εξετάσαμε τις ευπάθειες και απειλές της, τα μέτρα ασφαλείας της και τις καλές πρακτικές ασφαλείας της αρχιτεκτονικής της. Ένας άλλος τρόπος υλοποίησης της εικονικοποίησης (virtualization) είναι με την τεχνική operating system level virtualization, στην οποία κυρίαρχο ρόλο παίζουν τα containers.

Ως μελλοντική εργασία, λοιπόν, προτείνεται η διεξαγωγή ανάλογης έρευνας για την μελέτη και καταγραφή των ευπαθειών και απειλών, των μέτρων ασφαλείας και των καλών πρακτικών ασφαλείας της αρχιτεκτονικής

για την υλοποίηση της εικονικοποίησης (virtualization) με την τεχνική operating system level virtualization ή containers. Γνωστές τεχνολογίες υλοποίησης της εικονικοποίησης με την τεχνική των containers είναι οι Docker, Solaris Containers, OpenVZ, Linux-VServer, LXC, AIX Workload Partitions, Parallels Virtuozzo Containers και iCore Virtual Accounts.

Βιβλιογραφία

[1] https://el.wikipedia.org/wiki/Εικονικοποίηση.

[2] MICHAEL PEARCE, The University of Canterbury, SHERALI ZEADALLY, University of The District of Columbia, RAY HUNT, The University of Canterbury. Virtualization: Issues, Security Threats, and Solutions. ACM Computing Surveys, Vol. 45, No. 2, Article 17, Publication date: February 2013.

[3] Κωνσταντίνα – Κρίνα Βλαχάκη, Πανεπιστήμιο Πατρών. Συγκριτική μελέτη Openstack με VMware: Προτάσεις για επέκταση των προσφερόμενων υπηρεσιών. Φεβρουάριος 2016.

[4] NIST: http://dx.doi.org/10.6028/NIST.SP.800-145, SP 800-145. The NIST Definition of Cloud Computing. September 2011.

[5] https://en.wikipedia.org/wiki/Hypervisor.

[6] R. M. Sharma Assistant Professor, Department of Computer Application, MCNUJC, Bhopal Madhya Pradesh, India. The Impact of Virtualization in Cloud Computing. International Journal of Recent Development in Engineering and Technology, ISSN 2347-6435(Online) Volume 3, Issue 1, July 2014.

[7] VMware. Understanding Full Virtualization, Paravirtualization, and Hardware Assist. March 11, 2008.

[8] https://en.wikipedia.org/wiki/Virtualization.

[9] https://en.wikipedia.org/wiki/Application_virtualization.

[10] http://www.onecloudsol.com/virtualization.html.

[11] Cloud Security Alliance (CSA). Best Practices for Mitigating Risks in Virtualized Environments. April 2015.

[12] Karen Scarfone, Murugiah Souppaya, and Paul Hoffman. Guide to Security for Full Virtualization Technologies, Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-125, January 2011.

[13] Yuping Xing and Yongzhao Zhan, School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, China. Virtualization and Cloud Computing. Springer-Verlag Berlin Heidelberg 2012.

[14] Naveed Ahmad, Ayesha Kanwal and Muhammad Awais, Shibli National University of Science and Technology School of Electrical Engineering and Computer Science Islamabad, Pakistan. Survey on Secure Live Virtual Machine (VM) Migration in Cloud. 2nd National Conference on Information Assurance (NCIA), 2013.

[15] Ivan Studnia, Eric Alata, Yves Deswarte, Mohamed Kaaniche, Vincent Nicomette. Survey of Security Problems in Cloud Computing Virtual Machines. Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012). Cloud and security: threat or opportunity, <hal-00761206>, Nov 2012.

[16] https://en.wikipedia.org/wiki/Hyperjacking.

[17] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, Computer Science & Software Engineering, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia. Emerging Security Challenges of Cloud Virtual Infrastructure. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[18] Candid Wueest, Symantec. Security Response, Threats to virtual environments. Version 1.0 – August 12 2014.

[19] Trend Micro. Virtualization and Cloud Computing: Security Threats to Evolving Data Centers.

[20] Sarfraz Nawaz Brohi, Mervat Adib Bamiah, University Technology Malaysia, Muhammad Nawaz Brohi, Rukshanda Kamran Preston University Ajman, UAE. Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures. Proceedings of 2012 International of Cloud Computing, Technologies, Applications & Management, IEEE 2012.

[21] CA Technologies. Top virtualization security risks and how to prevent them. SearchSecurity.com E-Guide.

[22] Muhammad Kazim, Rahat Masood, Muhammad Awais Shibli, and Abdul Ghafoor Abbasi National University of Sciences and Technology, Sector H-12, Islamabad - 44000, Pakistan. Security Aspects of Virtualization in Cloud Computing. IFIP International Federation for Information Processing 2013.

[23] Kanika M. Tech. Research Scholar, Navjot Sidhu Assistant Professor, Centre for Computer Science and Technology Central University of Punjab Bathinda, India. Analysis of Virtualization: Vulnerabilities and Attacks over the Virtualized Cloud Computing. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 2014.

[24] https://el.wikipedia.org/wiki/ARP_spoofing.

[25] Eduardo B. Fernandez Department of Computer and Electrical Engineering and Computer Science Florida Atlantic University Boca Raton FL USA, Raul Monge Departament of Informatics Universidad Tecnica Federico Santa Maria Valparaiso Chile, and Keiko Hashizume. Building a security reference architecture for cloud systems. Received: 30 June 2014 / Accepted: 17 December 2014 / Published online: 6 January 2015, Springer-Verlag London 2015.

[26] Pooja Kedia Amity University Noida, Uttar Pradesh, Renuka Nagpal Amity University Noida, Uttar Pradesh and Tejinder Pal Singh JK Technosoft Noida, Uttar Pradesh. A Survey on Virtualization Service Providers, Security Issues, Tools and Future Trends. International Journal of Computer Applications (0975 – 8887) Volume 69– No.24, May 2013.

[27] Ioannis Chatzikyriakidis, Kingston University, Faculty of Computing, Information Systems & Mathematics Tei of Piraeus, Departments of Electronics and Automation. Trends And Risks in Virtualization, Dissertation submitted for the Degree of Master of Science in Networking and Data Communications. JULY 2011.

[28] https://en.wikipedia.org/wiki/Virtual_firewall.

[29] https://www.veracode.com/security/spoofing-attack.

[30] VMWARE-SAVVIS. Securing the Cloud: A Review of Cloud Computing, Security Implications and Best Practices. WHITE PAPER.

[31] VMWARE. Security of the VMware vSphere Hypervisor. JANUARY 2014.

[32] VMWARE. vSphere Security ESXi 6.0 vCenter Server 6.0. EN-001466-04. Copyright 2009–2015 VMware.

[33] https://en.wikipedia.org/wiki/Hardware_virtualization.

[34] http://cloudacademy.com/blog/container-virtualization.

[35] https://www.dwheeler.com/essays/cloud-security-virtualization-containers.html.

[36] K.Mani, Associate Professor, Department of Computer Science, Nehru Memorial College, Puthanampatti, India and R.Mohana Krishnan, Research Scholar, Department of Computer Science, Nehru Memorial College, Puthanampatti, India. A Survey on Cloud Computing Virtualization. International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801 ISSN (Print): 2320-9798, Vol. 4, Issue 5, May 2016.

[37] Brona Shah, Jignesh Vania, Department of Computer Engineering, Gujarat Technological University, Gujarat, India. A Literature Survey on Virtualization Security Threats in Cloud Computing. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358, Volume 3 Issue 12, December 2014.

[38] Leonardo Richter Bays, Rodrigo Ruas Oliveira, Marinho Pilla Barcellos, Luciano Paschoal Gaspary and Edmundo Roberto Mauro Madeira, Institute of Informatics, Federal University of Rio Grande do Sul, Porto Alegre, Brazil. Virtual network security: threats, countermeasures, and challenges. Journal of Internet Services and Applications, Springer 2015.

[39] CLOUD SECURITY ALLIANCE. The Treacherous 12 - Cloud Computing Top Threats in 2016. February 2016.

[40] Amani S. Ibrahim, James Hamlyn- Harris and John Grundy, Computer Science & Software Engineering, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia. Emerging Security Challenges of Cloud Virtual

Infrastructure. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[41] http://cd83.net/vmware-vcenter-server-appliance-vs-vcenter-for-windows-managing-your-esxi-environment/.

[42] http://www.mimastech.com/2016/06/24/introduction-to-server-virtualization-technology/.

[43] http://www.bitdefender-my.com/new-memory-introspection.html.

[44] http://addo.systems/private-virtual-environment/.

[45] http://www.telecom-cloud.net/network-as-a-service/.

[46] http://www.rishabhsoft.com/blog/7-superb-benefits-of-saas.

[47] https://www.zoho.com/creator/paas.html.

[48] http://www.cloudhosttechnologies.com/resources/cloud-iaas/.

[49] http://codelogic.tumblr.com/post/88655058783/interesting-titbit-about-hyper-v.

[50] http://codelogic.tumblr.com/post/88655058783/interesting-titbit-about-hyper-v.

[51] https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphere.server_configclassic.doc_40/esx_server_config/security_for_esx_systems/c_security_and_virtual_machines.html.

[52] http://www.vmware.com/techpapers/2007/understanding-full-virtualization-paravirtualizat-1008.html.

[53] http://www.vmware.com/techpapers/2007/understanding-full-virtualization-paravirtualizat-1008.html.

[54] http://www.vmware.com/techpapers/2007/understanding-full-virtualization-paravirtualizat-1008.html.

[55] http://www.private-cloudcomputing.com/sale-7709660-distributed-government-cloud-computing-desktop-virtualization-vdi-vs-os-streaming.html.

[56] https://en.wikipedia.org/wiki/Application_virtualization.

[57] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html.

[58] http://www.onecloudsol.com/virtualization.html.

[59] http://www.anandtech.com/show/2480/10.

[60] http://wwpi.com/2016/08/26/combating-file-sharing-data-leakage/.

[61] http://www.icym.edu.my/v13/about-us/our-news/general/580-denial-of-service-attack.html.

[62] https://gr.pinterest.com/virusolutions/remove-pc-virus/.

[63] http://www.cs.wustl.edu/~jain/cse571-11/ftp/virtual/index.html.

[64] https://en.wikipedia.org/wiki/Hyperjacking.

[65] https://trtpost-wpengine.netdna-ssl.com/files/2013/12/shutterstock_148642874-680x400.jpg.

[66] http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html.

[67] http://www.123rf.com/photo_24308594_stamp-with-text-out-of-date-inside-vector-illustration.html.

[68] https://www.cbinsight.com/as-online-data-theft-escalates-banks-look-to-retailers-to-bear-the-losses.html.

[69] http://radhanathswamiinspires.com/quote/radhanath-swami-says-to-fail-is-not-much-of-a-loss/.

[70] https://www.teachprivacy.com/sensitive-data-different-definitions-privacy-law/.

[71] http://sociable.co/data/what-companies-need-to-start-doing-to-keep-their-customers-safe-from-data-theft-2/.

[72] https://www.dreamstime.com/stock-illustration-high-level-security-safety-gradation-concept-computer-firewall-settings-web-interface-app-switch-button-image65459491.

[73] http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html.

[74] http://betanews.com/2015/12/30/state-sponsored-hackers-microsoft-account/.

[75] http://computersecuritypgp.blogspot.gr/2015/09/how-to-detect-arp-spoofing-attack-in.html.

[76] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm.

[77] https://jon.oberheide.org/blog/2008/02/10/exploiting-live-virtual-machine-migration/.

[78] https://blogs.vmware.com/management/2013/12/the-savings-potential-of-automated-resource-reclamation-part-1.html.

[79] https://www.shutterstock.com/image-illustration/security-policy-word-tag-cloud-on-195043955.

[80] http://www.secure-bytes.com/hardening-services.php.

[81] http://www.websnatchsoftware.com/being-prepared-with-it-disaster-recovery-plan.html.

[82] http://www.kenia.ahk.de/information/events/events-detail/artikel/civil-security-technologies-and-services-june-2015/?cHash=f3af1761b82b223d8dfa39cdf8ad7df8.

[83] http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2011/no3_1_1/articles/201105/t20110520_235160.html.